A Survey on Emerging SDN and NFV Security Mechanisms for IoT Systems

Ivan Farris, Tarik Taleb, *Senior Member, IEEE*, Yacine Khettab, and Jaeseung Song, *Senior Member, IEEE*

***Abstract*—The explosive rise of Internet of Things (IoT) systems have notably increased the potential attack surfaces for cybercriminals. Accounting for the features and constraints of IoT devices, traditional security countermeasures can be inefficient in dynamic IoT environments. In this vein, the advantages introduced by software defined networking (SDN) and network function virtualization (NFV) have the potential to reshape the landscape of cybersecurity for IoT systems. To this aim, we provide a comprehensive analysis of security features introduced by NFV and SDN, describing the manifold strategies able to monitor, protect, and react to IoT security threats. We also present lessons learned in the adoption of SDN/NFV-based protection approaches in IoT environments, comparing them with conventional security countermeasures. Finally, we deeply discuss the open challenges related to emerging SDN- and NFV-based security mechanisms, aiming to provide promising directives to conduct future research in this fervent area.**

***Index Terms*—Internet of Things, security, SDN, NFV, cloud, edge computing.**

I. Introduction

THE ADVANCEMENT of the Internet of Things (IoT) paradigm can bring remarkable transformation in each domain of human life. A myriads of smart devices will make our environments smarter by enabling sensing and actuation capabilities, contextual awareness, and physical-virtual bridging. To achieve these goals, IoT devices are able to interconnect and to jointly provide services also assisted by back-end systems, for example, when processing the huge amount of data generated by sensing activities [1]. Devices can also take autonomous decisions by perceiving the surrounding context and provide real-time information to users, thus improving decision support systems. All these envisioned benefits are boosting the adoption of IoT devices as key assets along the value service chain.

On the other hand, IoT systems can introduce new potential attack surfaces to be exploited by malicious cybercriminals. If not appropriately considered, IoT security threats can bring tremendous economical and reputation damages, thus undermining the widespread adoption of IoT. In industrial ecosystem, attacks against smart IoT appliances can cause interruption in production workflows and, even worse, compromise the quality of products. IoT devices used in home and health-care environments carry on sensitive user information. Therefore, flaws in data integrity and confidentiality can cause critical information leakage. Furthermore, the multitude and heterogeneity of IoT, ranging from smart cars to resource-constrained devices (e.g., sensors and actuators), from industrial robots to personal smart-watches, magnify the complexity of managing the security mechanisms in a uniform way, especially for non-savvy users. Accounting for the native connectivity capabilities of IoT devices, the misconfiguration of defense systems for a single node represents the weakest link of the chain, thus introducing the risk to compromise the interconnected devices and the relevant service outcomes. The analysis of security for IoT systems requires a systematic and comprehensive approach accounting for the manifold attack surfaces.

The constraints and heterogeneity of IoT systems make classic solutions, such as static perimeter defenses and device-host security mechanisms, unsuitable for extremely dynamic IoT environments, thus requiring novel network-based protection strategies to enforce security in a scalable and effective way [2]. Indeed, notable efforts have been addressed over the last years to design next-generation Internet architectures [3], embracing the concept of security and privacy by design. In this vein, network softwarization represents a breakthrough in Telco industries, by bringing several advantages in terms of flexibility and manageability [4]. This transformation is leaded by Software Defined Networking (SDN) and Network Function Virtualization (NFV) paradigms [5]. The former aims at increasing network programmability by leveraging the separation of control and data planes, whereas the latter boosts the development of virtualized network appliances to be executed on top of commodity servers [6]. Even in the context of network security, SDN and NFV are gaining high momentum, representing key enablers towards the on-demand provisioning of protection mechanisms, according to the SECurity-as-a-Service (SECaaS)

Manuscript received August 7, 2017; revised February 19, 2018 and June 13, 2018; accepted July 2, 2018. Date of publication August 1, 2018; date of current version February 22, 2019. This work was supported in part by the ANASTACIA Project through the European Unions Horizon 2020 Research and Innovation Programme under Grant 731558, and in part by the Swiss State Secretariat for Education, Research, and Innovation. The work of J. Song was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant NRF-2017R1D1A1B03036285. *(Corresponding author: Tarik Taleb.)*

I. Farris and Y. Khettab are with the Department of Communications and Networking, School of Electrical Engineering, Aalto University, 02150 Espoo, Finland (e-mail: ivan.farris@aalto.fi; yacine.khettab@aalto.fi).

T. Taleb is with the Department of Communications and Networking, School of Electrical Engineering, Aalto University, 02150 Espoo, Finland, and also with the Computer and Information Security Department, Sejong University, Seoul 143-747, South Korea (e-mail: tarik.taleb@aalto.fi).

J. Song is with the Computer and Information Security Department, Sejong University, Seoul 143-747, South Korea (e-mail: jssong@sejong.ac.kr).

Digital Object Identifier 10.1109/COMST.2018.2862350

model [7]. These novel SDN/NFV-based security mechanisms can better cope with IoT security threats, especially accounting for the increasing blurring between physical and virtual IoT ecosystems.

In this survey, we aim at presenting a detailed analysis of SDN/NFV-based security mechanisms to increase the protection of IoT systems, pointing out introduced advantages and potential application scenarios. To this aim, we first provide a systematic study of security threats of IoT domains, especially highlighting the additional requirements introduced by IoT environments. The background analysis is completed by a brief description of main conventional security approaches for IoT security, focusing on authentication, encryption, access control, and detection solutions. Then, we provide an extensive analysis of security mechanisms provided by SDN and NFV, including a detailed background behind these promising network paradigms and current integration efforts into IoT systems. Our survey represents the first work in the literature to systematically investigate the joint usage of SDN- and NFV-based security mechanisms in the complex and heterogeneous landscape of IoT systems. To this aim, the main security features are identified, presenting a comprehensive overview of SDN/NFV-based security solutions and relevant application scenarios at different levels, such as in cloud, core, and access IoT networks. This analysis includes comparison with conventional security solutions, allowing to highlight the advantages as well as the complementarity in manifold IoT environments, and to derive the lessons learned so far.

Since our literature review shows that the research in this area is still incipient, we believe that another key contribution of this survey is represented by a detailed discussion on future research directions towards the broad deployment of SDN/NFV-based security solutions. To this aim, we have identified the following open challenges: definition of security IoT policies, orchestration over heterogeneous IoT domains, inherent security of SDN and NFV systems augmented by IoT devices, optimal selection and deployment of SDN/NFV-based security mechanisms, and security granularity for IoT network slicing. We believe that this survey can provide extensive guidelines for new researchers who would like to explore this fervent area.

A. Comparison With Surveys on IoT Security

In the literature, different surveys have broadly analyzed IoT systems, also addressing relevant security challenges. In [1], the main technology enablers of IoT systems are described, also identifying open security and privacy aspects. Hossain *et al.* [8] provide an analysis of security vulnerabilities for IoT systems, with a three dimensional framework to indicate the intricacy of IoT security domain; however, the analysis of existing countermeasures is missing. In [9], security and privacy threats relevant to IoT are discussed only on a legislative point of view. An overview of security solutions for IoT systems is provided in [10]. However, new emerging SDN/NFV-based security models are not discussed therein. Furthermore, remarkable efforts have been carried out over the past years for securing Wireless Sensors Networks [11]–[13] and Radio Frequency Identification (RFID) systems [14], [15]. However, several doubts have been raised with relevance to the effective applicability of WSN/RFID-oriented security mechanisms for IoT environments. Other surveys discuss specific security solutions for IoT domains, such as authentication [16], [17], detection systems [18], thus focusing on narrow range solutions and lacking a global vision. In Table I, we provide an analysis of previous literature surveys on security countermeasures for IoT, showing that an extensive study of SDN/NFV-based security countermeasures to cope with IoT attacks is currently missing. Our survey aims to fill this gap presenting the potential of SDN/NFV-based security solutions to secure IoT systems.

Other surveys have investigated the security features related to SDN and NFV paradigms. In [23]–[25], SDN-based security solutions are proposed to enhance network protection. Several works have also investigated the inherent security challenges introduced by SDN [26], [27], illustrating potential countermeasures. On the other hand, NFV can impact the security of virtualized networks, whose challenges have been analyzed in [28] and [29]. To cope with security threats in the NFV infrastructure, several best security practices are described in [30]. However, all the above-mentioned works separately present SDN and NFV-based security mechanisms, thus an integrated vision is missing. Furthermore, these works lack to specifically address the peculiar features and threats of IoT systems.

B. Organization of the Paper

The rest of this paper is structured as follows. Section II briefly presents the main features of IoT systems according to a three layer taxonomy, whereas Section III analyzes relevant security threats. Section IV provides an overview of main conventional security countermeasures against IoT attacks. In Sections V and VI, we respectively present SDN and NFV paradigms in a comprehensive manner, analyzing integration approaches with IoT systems, and especially focusing on their security features. Section VII derives lessons learned in the adoption of SDN/NFV-based security solutions in IoT environments, comparing them with conventional security countermeasures. Section VIII thoroughly discusses open research areas, whereas concluding remarks are drawn in Section IX.

II. Overview on IoT Landscape

In this section, we provide an overview of current IoT landscape, considering end-to-end solutions from devices to relevant IoT applications. In our analysis, we take into account how the broad adoption of cloud technologies, up to the extreme edge of the network, is making the borders even more blurry between network environments and IoT cloud-based platforms [31]. In this vein, we have opted for a three layer taxonomy, including IoT devices, IoT-oriented cloud networks and platforms, and IoT applications. In the following, we describe each domain, illustrating its main features and its enabling technologies.

TABLE I
PREVIOUS SURVEYS ON SECURITY COUNTERMEASURES FOR IOT

Survey	Security Aspects							Year
	Authentication	Encryption	Access Control	Detection	Privacy	SDN	NFV	
Sicari et al. [10]	YES	YES	YES	NO	YES	NO	NO	2015
Granjal et al.[19]	YES	YES	YES	NO	NO	NO	NO	2015
Saadeh et al.[16]	YES	NO	NO	NO	NO	NO	NO	2016
Nia et al. [20]	YES	YES	YES	NO	YES	NO	NO	2016
Ferrag et al. [17]	YES	NO	NO	NO	NO	NO	NO	2017
Zarpelao et al. [18]	NO	NO	NO	YES	NO	NO	NO	2017
Yang et al. [21]	YES	YES	YES	NO	YES	NO	NO	2017
Alaba et al. [22]	YES	YES	YES	NO	YES	YES	NO	2017

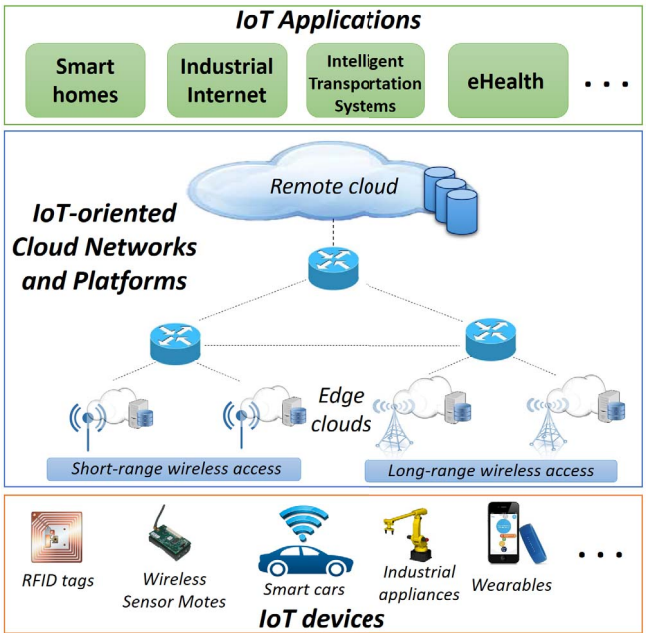


Fig. 1. IoT Overview.

A. IoT Device Layer

This layer includes the devices able to interact with the physical environments, by leveraging identification, sensing, and actuation capabilities. Through their pervasive capabilities, IoT devices represent the bridge between the physical and cyber domains. The main technologies adopted in this layer are RFID technologies and Wireless Sensor Networks (WSNs). The main application scenario for RFID tags deals with the identification and tracking of goods [32]. Therefore, RFID tags present extremely low costs and can be battery-free by leveraging electromagnetic energy harvesting [33]. WSNs have been used in manifold application scenarios, such as environmental monitoring, agriculture, military scenarios, and smart cities, and represent a key enabler for IoT adoption [34].

We finally remark that by leveraging the reduction costs of enabling identification and sensing modules, these components are nowadays embedded in a great variety of smart devices, such as autonomous vehicles [35], industrial robots [36], and Unmannered Areal Vehicles (UAVs) [37], [38]. This trend exponentially increases the number of potential devices involved in IoT solutions, further boosting the attraction of cybercriminals to exploit vulnerabilities and launch massive attacks.

B. IoT-Oriented Cloud Networks and Platforms

The increased connectivity of smart objects has given impetus towards the explosion of IoT paradigm. Several communication strategies and networking schemes have been specifically designed to meet the requirements of sensing and actuation devices, accounting for their resource constraints and limited battery energy supply. The desire to provide global interconnectivity for each object has boosted notable efforts of IETF community to design and develop an IPv6-based protocol for IoT nodes [39]. Furthermore, accounting for the massive number of devices and the expected huge amount of traffic, cloud technologies have been envisioned as core enabler for IoT solutions. Also, to better cope with low-latency IoT applications, the Edge computing paradigm is boosting the deployment of micro data centers at the edge of the network [40]. Last but not the least, IoT service layer platforms have been standardized to provide common IoT service functions, such as device management, group management, security, and global discovery [41]. In the next sections, we provide an overview of these trends, which have notable impact on the relevant security of IoT solutions.

1) IPv6-Based IoT Protocol Stack: The physical and link layer technologies have been designed to support constrained IoT devices, thus presenting low energy consumption and low transfer rates. Regarding short-range wireless communication protocols for WSN, IEEE 802.15.4 [42], IEEE 802.11ah, and Bluetooth Low Energy (BLE) [43] are the most widely adopted solutions. Furthermore, over the last years, Low Power wide Area Networks (LPWAN) technologies have attracted the interest of research and industrial communities, boosted by SigFox, Lora, and cellular-based solutions (e.g., Narrowband IoT) [44]. Indeed, upcoming 5G systems are considered potentially key drivers to further boost the widespread of IoT by developing solutions able to accommodate relevant requirements [45], [46].

Accounting for the heterogeneity of access technologies, the main challenge represents the global interconnectivity to ensure a uniform IoT networking. To this aim, several IETF

efforts have addressed the design of specific adaptation layers to enable different wireless technologies interconnectivity by leveraging IP networking: 6LoWPAN WG has specifically focused on IEEE 802.15.4; 6lo WG copes with a variety of short range protocols, such as BLE and NFC; and LPWAN has recently started to address the challenge for long-range IoT communications. Another crucial step towards a standardized protocol stack for IoT has dealt with the development of specific application protocols. In this vein, accounting for the complexity of HTTP, a lightweigth RESTful application protocol, Constrained Application Protocol (CoAP) [47], has been proposed to support efficient interactions even with resource-constrained IoT devices.

2) Cloud and Edge Computing: Accounting for the on-demand resource provisioning enabled by virtualized environments, cloud technologies represent a key solution to cope with the scalability issues due to the massive spread of IoT devices [31]. To provide the virtualized resources required to execute applications, three different virtualization layers have been devised: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Indeed, several cloud-based platforms have been proposed over the last years from both research projects and industrial communities [48], [49].

Nowadays a great variety of IoT solutions are demanding for strict latency requirements. In this vein, the Edge computing paradigm [40] is rapidly gaining momentum, promoting distributed small-scale cloud environments deployed at the edge of the network to execute applications near to the IoT devices. This approach can introduce several benefits by: (i) ensuring low-latency application response times; (ii) reducing network traffic overhead, since data generated by IoT devices can be processed at the edge avoiding traffic forwarding to remote cloud data centers; (iii) providing context data awareness for location-based services. ETSI Multi-Access Edge Computing (MEC) and OpenFog consortium are leading the standardization and broad adoption of edge computing solutions. Several IoT systems have fully embraced the Edge computing paradigm [50]–[52], by developing new models to split data processing between the edge and the cloud. Furthermore, the rise of lightweight virtualization technologies, such as LXC and Docker containers [53], allows even resource-constrained device to host IoT services [54].

C. Applications Layer

This layer includes all the application modules required to provide the desired IoT service to the end-users. Indeed, accounting for the manifold application scenarios, IoT platforms greatly differ to accommodate specific business logic requirements. The most promising usage concerns smart home automation [55], Industrial Internet [36], intelligent transportation systems [56], smart energy [57], enhanced health-care services [58], and smart cities [59].

III. Security Threats in IoT Environments

This section aims to provide a comprehensive analysis of attack threats in IoT environments. Based on the IoT taxonomy presented in the previous section, the security threats are discussed in-depth for each domain.

A. Security Attacks on IoT Devices

Accounting for the constrained computation capabilities and limited energy supply of IoT devices, the adoption of conventional strong security mechanisms is not guaranteed, thus increasing the potential vulnerabilities. In addition, IoT devices can operate remotely and unattended by human intervention, thus making them vulnerable to physical attacks. We remark that attacks against the physical devices can be extremely dangerous in IoT systems, since the compromised nodes can generate altered measurements. As a result of the corrupted information, IoT control systems can be severely impacted, providing erroneous feedback information and wrong services. In the following, we describe the main attacks related to the IoT device layer.

1) Hardware Trojan Attack: Trojans have emerged as a major security concern for IoT devices [20]. Trojan is a malicious modification of hardware, which allows the attacker to exploit the infected IoT device to gain access to either sensitive data or software running on that device. To this aim, the attacker alters the original circuitry during design or fabrication and inserts a triggering mechanism that activates the malicious behavior of the Trojan [20].

2) Replication Attack: A malicious attacker can create a new node by replicating the sensitive identification information of a target device. Then, to allow the connectivity to the existing IoT system, the replicated node is faked as authorized, generating severe vulnerabilities in the IoT system. Indeed, the node can generate false data, making IoT applications returning erroneous feedback commands or providing wrong processed information. Furthermore, the replicated node can also enable the attacker to obtain security privileges, such as extracting cryptographic shared keys [60], and to revoke authorized nodes by carrying out node revocation mechanisms [61].

3) Tampering Attacks: IoT devices can operate remotely and unattended by human intervention, thus making them vulnerable to tampering attacks. Tampering attacks refer to all scenarios where a malicious entity performs an unauthorized physical or electronic action against the device. The adversary can exploit the physical access to the device to gain full control, therefore known also as *node capture attacks*, causing intentional malfunction or sabotage [62]. In [63], an extended analysis of tampering attacks on sensor node is provided, especially focusing on the malicious approaches which can be executed in the deployment area, without interruption of the regular node operation.

4) Battery Draining Attacks: The majority of wireless sensor and actuator devices relies on embedded small batteries with limited energy capacity. This features can be exploited by malicious attackers to make an IoT device unavailable by completely draining its battery. This attack can be performed by sending a huge number of packets to the target devices, forcing their processing and the relevant resource consumption, which can rapidly consume the available energy [64].

Since IoT nodes typically use advanced duty cycle mechanisms to extend their lifecycle, a cyber-criminal can launch an attack, also known as sleep deprivation, to alter the normal sleep routing and force the target node to be awake until the complete depletion of its energy [65]. These battery-draining attacks can have severe consequences on IoT systems since the services provided by a single or a group of devices become interrupted, potentially causing the inefficiency of the whole IoT solution, such as a fire detection system.

5) Malicious Code Injection Attacks: In addition to hardware tampering attacks, attackers can take control of a device by injecting malicious code into its memory [66]. The injected malicious code can alter the normal node behaviour and can be even exploited to grant the adversary with increased privileges in the associated IoT system.

B. Security Threats in IoT-Oriented Cloud Networks and Platforms

IoT-oriented cloud networks and platforms represent a crucial domain of IoT systems, not only providing the connectivity between IoT devices and relevant applications, but also offering the computation and storage capabilities of cloud environments to execute distributed IoT platforms. Therefore, potential vulnerabilities in this domain can have tremendous consequences, severely impacting the correct behavior of IoT solutions. In the following, we provide an in-depth description of attacks in IoT-oriented cloud networks and platforms.

1) Eavesdropping Attack: Eavesdropping (also known as data sniffing) is a potential cyber-attack performed by intentionally listening to private IoT communications. When data are transmitted unencrypted, the adversaries can obtain sensitive information, such as credential or node configuration.

2) Denial-of-Service Attack: Denial-of-Service (DoS) attack is one of the most common networking attacks and can have dramatic impact against IoT systems: by attacking and compromising the communication links, as well as flooding IoT networks with massive data, DoS attacks can rapidly exhaust resources causing the unavailability of IoT systems. Since the majority of IoT devices use wireless communication links, interference and jamming attacks can be used to block radio transmissions. Jamming attacks can be continuous [67], thus causing full or intermittent dis-connectivity [68], to lower the performance of time-sensitive IoT services. On the other hand, the flooding of IoT networks can have serious consequences over the IoT systems availability. Different approaches can be used to carry out DoS attacks, such as Ping of Death, TearDrop, UDP/SYN flood, and SYN flood. Furthermore, the effects of these attacks get notably increased when they are performed in a distributed way, i.e., Distributed DoS (DDoS). In this vein, the vulnerabilities of IoT devices can be exploited to create large-scale botnets and to launch massive DDoS attacks [69].

3) Spoofing Attack: The objective of spoofing attacks is to generate and send malicious packets that seem legitimate in the IoT systems. This malicious approach can be used in IP-based IoT systems, where the adversary can spoof the IP addresses of authorized IoT devices. Then, the adversary can send malicious data with the spoofed IP addresses, making relevant communication legitimate, thus gaining access to the IoT system [70]. In case of RFID solutions, the attacker can record the information of a valid RFID tag and then generates altered information using the valid tag ID [71].

4) Man-in-the-Middle (MitM) Attack: The MitM attack is an advanced version of spoofing attack wherein a malicious entity is on the network path between two IoT communicating devices. The adversary impersonates both endpoints and makes independent connections with each target, to intercept the exchanged traffic, and then transfers and forwards messages between them. In this way, the adversary is capable of delaying, cloning, replaying, spoofing or dropping packets. Impersonation makes the endpoints believe that they are talking directly to each other, while the entire conversation is controlled by the attacker. Reliable information, such as sensitive health status, industrial IoT control feedback, or even secret keys of house doors, can be forged and altered by an attacker with MitM, thus causing serious IoT security issues [22].

5) Routing Attacks: Routing attacks manipulate routing control information to alter how packets are routed over IoT networks. In this way, malicious adversaries can create routing loops or generate false error routing messages. Different strategies have been investigated to carry out routing attacks. In a Black Hole attack, a malicious node advertises the shortest path to a destination node, so that all packets are routed towards itself. Then the adversary can drop or alter the incoming packets [72]. In a Hello Flood attack, a broadcast "Hello Packet" from a malicious node is used to advertise its presence to neighbors using high transmission power. The receiving nodes assume to be in the communication range of the sender, which can be selected as a next hop in the route, causing an unstable state in the network [73]. In a Sybil attack, an adversary device, i.e., a Sybil node, can claim legitimate identity in the IoT network and generate false routing information that can alter the correct forwarding rules of neighboring nodes [74].

6) IoT Cloud Service Manipulation: IoT services are deployed over cloud data centers according to different models, i.e., IaaS, PaaS, or SaaS. A cloud/edge data center that is controlled by a malicious administrator can generate a serious situation since the adversary can easily launch attacks against the deployed virtualized service instances, either VMs or containers. In this way, the attacker can have remarkable benefits: extracting sensitive information gathered by associated IoT devices; manipulating processing IoT data tasks, thus compromising potential critical closed-loop controls; infecting the services with malicious software and fake information, which can compromise the security of both local and remote entities, such as other connected services deployed over different cloud/edge data centers or associated IoT devices.

7) Privilege Escalation: A typical feature of IoT platforms is the resource sharing where data, generated by multiple IoT systems, are processed and stored by a common module, by leveraging appropriate isolation mechanisms. Similarly, cloud/edge data centers provide computing and storage resources for the deployment of IoT services over the same

physical/virtual infrastructure. In this vein, malicious services can launch privileged escalation attacks by exploiting potential vulnerabilities in the virtualization/isolation technologies. The potential outcomes can be extremely severe such as stealing sensitive information and even taking control of other services within the data center environment.

8) Security Inter-Working: As multiple IoT platforms are now being inter-worked, their security mechanisms should be consistent across the interconnected IoT platforms. Unfortunately, not many IoT platforms are using the same security mechanisms. For example, it is very common to see that an IoT platform A is using Oauth as a security key management mechanism while an IoT platform B is using a proprietary security solution which has different access rights and key management mechanisms. Such inconsistencies of security mechanisms on inter-worked systems can cause various security flaws such as privacy data leakage and privilege escalation.

C. Security Threats in IoT Applications

The application layer implements the business logic to effectively exploit the capabilities of IoT devices. The relevant security challenges account for vulnerabilities in the developed software, relevant data, and attacks against the involved users.

1) Malicious Virus/Worm: IoT applications can be severely damaged through malicious viruses and worms, which can allow data leakage and compromise the correct behaviour of cyber-physical systems [75]. Furthermore, the self-propagation capabilities of worms can notably make the risk higher, extending the threats to other components of the systems, as well as to different IoT applications.

2) Application Data Leakage: Another concern in this domain involves privacy leakage, whereby sensitive information can be extrapolated by both cybercriminals and honest but curious adversaries. These sensitive information, generated by IoT devices for specific domains, can also contain application context information which can be exploited by malicious users not only for hacking the application itself, but also for carrying out further attacks [76]. For example, when real-time information from an electrical metering system is revealed, adversaries can infer the absence of people in the house based on power utilization statistics, making it ideal for burglary.

3) Service Logging Failure: Logging activities can be extremely beneficial to monitor the status of deployed services and to detect security attempts. To this aim, developers should appropriately record authentication events and application errors in the relevant log. Furthermore, compromised virtualized instances can intentionally generate huge amount of logs, which can impact the hypervisor logging analysis from other instances. Inefficient logging monitoring can limit the capabilities of implementing security controls in cloud/edge environments [77].

4) Malicious Scripts: Malicious scripts can severely impact software execution, allow sensitive data leakage, and alter the features of IoT solutions. The scripts can be usually executed over IoT application portals, e.g., in the form of Java attack applets and Active-x scripts, so to fool the customers accessing relevant services through Internet.

5) Phishing Attacks: By leveraging infected e-mails and phishing websites, adversaries can perform phishing attacks aiming to obtain the users' credentials for IoT applications. In this way, malicious accesses to the relevant devices and IoT platforms can be carried out.

6) Inconsistent Software Patches: A software patch, which is fixing security vulnerabilities and bugs, is very important to improve the quality, usability and performance of software. However, by the nature of IoT devices, it is not easy to apply software patches to all deployed IoT devices. In particular, IoT devices with low memories typically do not support an Over-The-Air (OTA) update feature. Inconsistency of software versions among the same IoT devices can cause misbehaviour of IoT applications. Finally, we shall point out that the multiplicity and diversity of IoT applications vary across markets, potentially introducing specific security requirements. Other surveys deeply discuss security features for precise IoT application domains, such as smart grids [78], [79], vehicular networking [80], and Industrial Internet [81], [82].

IV. Conventional Security Mechanisms in IoT Environments

In this section, we provide an overview on the main conventional security countermeasures for IoT systems. Our analysis focuses on the following areas: authentication and authorization, traffic filtering, encryption protocols, and detection systems.

A. Authentication and Authorization for IoT

Authentication is considered as a key security enabler allowing to cope with most common IoT threats, such as man-in-the-middle attacks, impersonation attacks, forging attacks, replay attacks and Sybil attacks. The majority of current IoT authentication protocols rely on mutual authentication, which refers to two or more IoT devices authenticating each other, providing privacy and data integrity. This can be based on (i) symmetric cryptography, which generates unique symmetric keys for each session based on a shared algorithm, and (ii) public cryptography, which uses a combination of public and private keys for each entity. Other authentication mechanisms in IoT can include biometric and username/password authentications [83], [84]. For a detailed analysis of authentication protocols for IoT systems, the interested reader may refer to [17].

In the following, we focus on the Authentication, Authorization, and Accounting (AAA) framework, which is dedicated for intelligent access control of resources and security policy enforcement [85]. Indeed, this framework offers protection against multiple vulnerabilities, such as insecure network services, insecure interfaces, and privacy concerns. Authentication is the process of proving the user's or device's ID. To this aim, the framework uses a combination of a username and a corresponding password. If the submitted credentials are correct, the server responds with a token which can be used for various operations. Each token is

mapped to a set of "authorized" actions which can be executed by the authenticated entity. The authorization determines whether the entity has permissions to perform certain tasks or access certain data (e.g., accessing IoT device data or turning on/off IoT devices). This policy enforcement technique can be either user-based or role-based, meaning that the access rights can be determined per-user or per group of users. Regarding accounting features, the AAA framework does not only enable the financial and commercial features, but it can also control the generated traffic, preventing massive usage of resources.

Samociuk and Adamczyk [86] implemented an AAA framework at the IoT gateway level, providing a secure private topology that can be implemented in smart cites. They have presented a thorough evaluation of the security, performance and energy consumption of the system. The results show a variety of new security features and negligible latency and energy consumption overhead.

B. Traffic Filtering and Firewalls

A firewall, also known as packet filter, is a network security appliance which analyzes incoming/outcoming packets, checking for matches to any of the pre-configured filtering rules, to either drop or forward the packets accordingly. Each rule can be defined using a diverse set of parameters, such as used protocol, incoming/outcoming ports, source/destination IP addresses, and zones. There are two types of firewalls: stateful and stateless firewalls. The key difference between them is that stateless firewalls do not keep track of traffic patterns and data flows, and are limited to statically analyze packets; stateful firewalls can observe traffic streams from end to end, monitoring the overall sessions [87].

Gupta *et al.* [88] implemented a system to secure a home IoT network against privacy breaches using firewalls. Their work consists of routing all traffic through a Raspberry Pi gateway which secures the communications of IoT devices with the cloud database. The relevant firewall is implemented at the gateway level (Raspberry Pi) using IPTables. Promising results are shown, demonstrating the capabilities of the system when dealing with different kinds of attacks such as IP spoofing, ICMP DoS attacks, SYN flood attacks and communication attempts from unknown identities. In a larger IoT network, this solution can suffer from potential scalability issues, due to the resource limitations imposed by the resource-constrained gateways, creating a bottleneck and a potential single point of failure.

C. Encryption Protocols

Data encryption mechanisms ensure data confidentiality and integrity in IoT systems, preventing attackers from eavesdropping and data tampering during transmission. Most cryptosystems are based on symmetric and asymmetric key management. Elliptic Curve Cryptography (ECC) is an asymmetric algorithm which has emerged as an attractive and efficient public-key cryptosystem. Hasan *et al.* [89] designed a lightweight ECC-based protocol for multi-agent IoT systems. Datagram Transport Layer Security (DTLS) is another communication protocol which relies on symmetric key management. Keoh *et al.* [90] presented an analysis of the DTLS protocol in the context of IoT and proposed a lightweight approach tailored to IoT devices, providing different robust security functionalities. Other cryptosystems include PKI (Public Key Infrastructure) which is an end-to-end authentication and key agreement mechanism whereby a trusted public entity stores digital certificates and verifies the identity of involved parties [91].

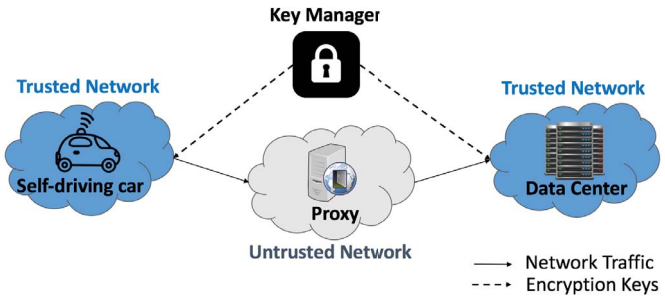


Fig. 2. Re-encryption using a Proxy.

The resource constraints of IoT devices can severely limit the effectiveness of the underlying encryption mechanisms. Deploying a proxy with re-encryption capabilities (using any of the aforementioned encryption approaches) represents a promising solution to address data integrity and confidentiality issues. Díaz-Sánchez *et al.* [92] proposed a proxy re-encryption solution between two endpoints exchanging data through an insecure network. The proxy acts as an intermediate node which resides between the two endpoints and it is responsible for re-encryption operations. The key manager is the entity which is in charge of mapping the destination public key using any addressing mechanism. For example, in the scenario shown in Fig. 2, all data coming from the self-driving car is sent to the proxy to be re-encrypted and forwarded to the data center. Both the self-driving car and the data center have public and private key pairs, and the key manager has both public keys.

D. Detection Systems

Intrusion Detection Systems (IDS) aim to detect unauthorized access and abnormal network traffic using either predefined attack patterns or signatures (Signature-based IDS) or the events log (Anomaly-based IDS). IDS are able to detect a wide range of attacks and abnormal network activities including: excessive bandwidth consumption, SYN flooding, ICMP DoS attacks, ARP spoofing attacks and even the use of a protocol with certain parameters defined by the administrator [93].

1) Signature-Based IDS: This type of IDS is based on a large library which consists of a pre-defined set of rules. If any (inbound or outbound) traffic matches with a rule, the IDS agent sends an alert to the security administrator, as sketched in Fig. 3. Although this static detection approach keeps false positives to a minimum, it requires detailed knowledge of each attack pattern and is not capable of discovering new types of attacks on its own.

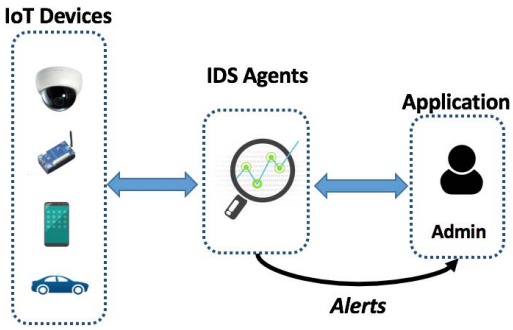


Fig. 3. A typical architecture of Intrusion Detection Systems in an IoT environment.

2) Anomaly-Based IDS: Unlike the signature-based approach, the anomaly-based IDS is event-driven. First, it defines the "normal" behavior of the network. Then, if any activity differs from the normal behavior, this event is considered as an intrusion. In order to accurately detect attacks and minimize the false alerts, this system uses artificial intelligence (AI) techniques. It thus needs to be trained to be able to classify network traffic [94].

A detailed survey on IDS solutions for IoT has been presented in [95], highlighting the key aspects to be considered in the design of a cross-platform distributed IoT approach. Accounting for the heterogeneous nature of IoT devices, the need for a unilateral intrusion detection support across different technologies is a pending research challenge. The authors also discussed the interoperability issues and the expected self-protection features for detection systems.

Another popular detection solution is represented by Deep Packet Inspector (DPI), which analyzes not only the packet header, but also its payload extracting the relevant signature. It operates at the seventh layer (the application layer) of the Open System Interconnection (OSI) protocol stack, and usually includes filtering capabilities. Each packet is classified according to a set of predefined rules. According to the system's decision, the packet can be either blocked, forwarded, or tagged for QoS (Quality of Service) purposes. A common practice is to forward the traffic to a honey-pot to further inspect the potential attack [96]. In the IoT context, new solutions which aim to design lightweight DPI systems are emerging. That is mainly due to the fact that IoT devices do not meet the computational requirements of existing DPI systems. Summerville *et al.* [97] designed a high-performance lightweight deep-packet anomaly detection solution which is feasible for such resource constrained devices. This approach uses "n-gram bit-patterns" to make a fast and efficient packet classification decision. Although the illustrated results show low level of false alerts and high efficiency, the authors have not evaluated the power consumption of this solution, which can be an issue for IoT systems.

V. SDN Security in IoT Environments

SDN is a promising network paradigm aiming at decoupling control and data planes to increase network programmability. In this way, SDN-based applications may have dynamic and granular access of network resources, and can specify traffic flow setting over the underlying infrastructure. This increased manageability of SDN-based networks allows the introduction of novel approaches to cope with security threats. Indeed, moving the network intelligence into the SDN controller introduces the opportunity to offload the complexity from network devices and to react fast in case of alerts by appropriately modifying traffic flows. In this section, we first provide a broad overview of SDN networking, particularly focusing on its adoption for IoT systems. Then, we describe the main security features of SDN networking aiming to achieve a major breakthrough in the protection of IoT systems.

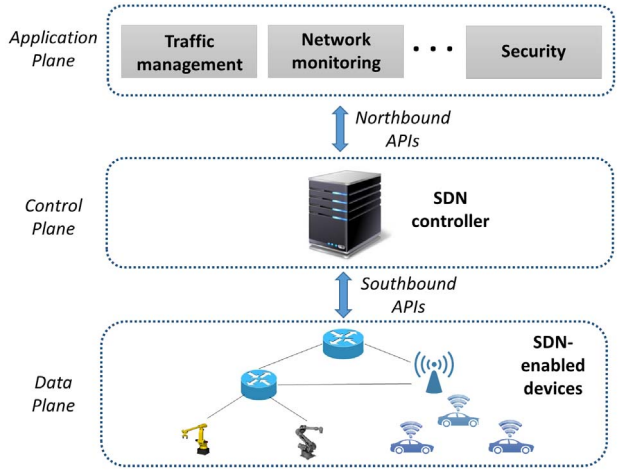


Fig. 4. The three layers in SDN architecture.

A. Background on SDN Adoption for IoT Systems

SDN guarantees enhanced network programmability by decoupling the control and forwarding functions. In this way, network management can be done separately, without affecting data flows, and can be carried out by a centralized controller. As a consequence, the complexity of the underlying switching devices is notably reduced in comparison with traditional networks. The derived SDN networks result into a simpler programmable environment, allowing external applications to define the network behavior. According to Open Networking Foundation (ONF), a non-profit consortium dedicated to development, standardization, and commercialization of SDN, the reference SDN architecture model [98] is composed of three layers, namely applications, control plane, and data plane (Fig. 4). The SDN applications can specify their requirements for the traffic management in the underlying networks through Northbound APIs. The SDN controller, which is in charge of the control plane, bridges the application plane and the data plane, translating applications' requirements into appropriate forwarding rules to be enforced by the underlying network switches. To this aim, the south-bound interface allows the SDN controller to access functions provided by the SDN-enabled switching devices. These functions may include reporting network status and managing packet forwarding rules. Indeed, the data plane includes network elements (e.g.,

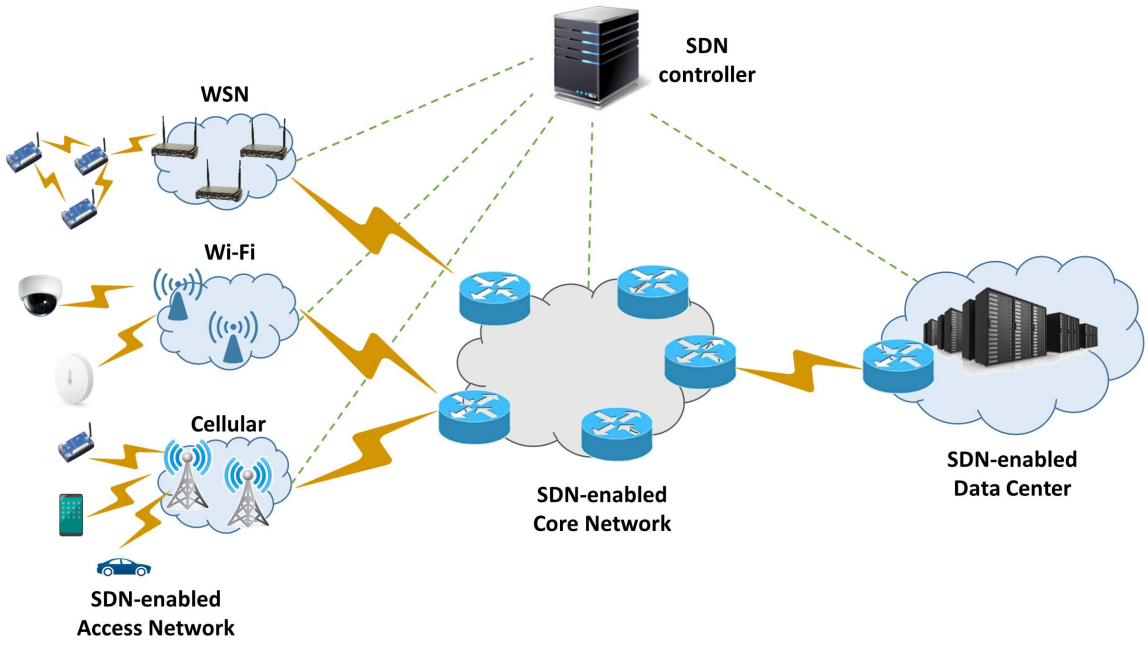


Fig. 5. Deployment scenarios of SDN paradigm for IoT systems.

switches and routers) which are exploited to process packets based on the rules provided by the SDN controller, and to collect network status information, such as network topology and traffic statistics. The adoption of standardized interfaces, e.g., Openflow, allows to increase interoperability among network elements, avoiding vendor lock-in issues.

Accounting for the increased manageability introduced by SDN, several works have investigated its integration for end-to-end IoT solutions. The adoption of SDN paradigm can be implemented at different levels, such as data center, core, and access networking, as illustrated in Fig. 5, thus covering the IoT traffic management from the devices, which generate the data, up to the cloud services, where data processing is performed. Each networking environment introduces specific requirements and optimization for the adoption of SDN, as deeply analyzed in [99]. Specific efforts are required for IoT access networks, aiming to provide unified network connectivity over wired and wireless networks [100]. Indeed, we remark how IoT is used as an umbrella term to include an extremely broad range of devices, ranging from low-constrained sensors adopted in WSN to autonomous cars, from smart home devices to industrial connected equipment. This has lead to the development of multiple IoT connectivity solutions, including short range meshed networks, typical of WSNs, and low-power cellular networks, where 5G is considered a fundamental enabler for IoT. In this variegated landscape, SDN represents a potential breakthrough in the efficient management of different IoT network environments due to its extreme flexibility and programmability. On the other hand, IoT domains introduce several challenges, in terms of latency, bandwidth, reliability, in-network data processing, and energy, which should be appropriately considered and require specific enhancements of SDN paradigm, as described in the following exemplary IoT scenarios.

Several exemplary case studies have addressed the adoption of SDN for vehicular communications, so to improve network utilization and ensure rapid network configuration [101], [102]. Indeed, accounting for the notable mobility of vehicles and latency requirements for safety drive applications, fast connection establishment and dynamic routing decisions require optimized strategies for SDN system over vehicular networks. In [103], an SDN-based architecture is also devised to specifically cope with constraints and features of WSNs, such as reducing the overhead of control traffic. TinySDN architecture [104] is proposed to enable multiple controllers for software-defined wireless sensor networks in TinyOS compatible devices. This approach transforms the wireless sensor nodes in an advanced entity including an SDN switch and an SDN end-device, called SDN-enabled sensor node. A peculiar feature of the TinySDN framework concerns the potential presence of multiple controllers within the WSN to reduce the overall latency. A stateful SDN solution, SDN-WISE, has been developed and tested for IEEE 802.15.4 in [105], able to enhance programmability of sensor nodes as finite state machines to enable a broad range of in-network operations. In [106], an enhanced SDN controller has been devised to ensure differentiated quality of service for IoT flows over heterogeneous IoT wireless networking scenarios. To ensure the seamless integration of SDN-WISE enhanced sensors and OpenFlow networks, the popular open-source ONOS framework [107] has been appropriately extended, as illustrated in [108]. By leveraging the increased features of the ONOS controller, two novel applications have been implemented to fully exploit the SDN capabilities of sensor devices: on the one hand, the SensorNodeForwarding application is in charge of installing the appropriate forwarding rules, based on the global topology, consisting of both OpenFlow and SDN-WISE nodes; on the other hand,

the SensorNodeDeviceManagement enables the remote sensor device management, therefore providing increased flexibility in the resource usage. Furthermore, an extensive performance analysis of SDN-based implementation for WSN has been conducted in [109], demonstrating that under static and quasi-static conditions, SDN outperforms two conventional protocols for IoT networks, i.e., ZigBee [110] and 6LoWPAN [111], independently of the network size, payload size, traffic generated, and considered performance metrics. Specific efforts have also addressed the adoption of SDN paradigm for Wi-Fi and cellular access IoT networks: in [112], a novel WiFi architecture, OPENSDWN, leverages SDN networking to provide datapath programmability and enable service differentiation and fine-grained transmission control, facilitating the prioritization of critical applications; an SDN-based flexible architecture for 5G cellular networks has been designed in [113] to fulfill functional and performance requirements of new generation services and IoT devices. The reader interested in aspects related to the integration of SDN networking with IoT systems can refer to these cited surveys [99], [114]–[116]. In our following analysis, we focus on the detailed analysis of SDN-based security mechanisms to enhance the protection of IoT systems.

B. SDN-Based Security Features for IoT

The use of SDN is gaining high momentum also within the security research communities. In this section, we provide an overview of the major SDN features which can be explored to provide advanced security mechanisms for IoT systems. For each envisioned feature, we provide a high-level explanation of the concept, deepening relevant solutions and exemplary implementations. This analysis also contains insightful findings related to the application of SDN-based security solutions in different IoT networking domains.

1) Traffic Isolation: SDN can be exploited to enable forwarding of different network traffics over the same physical network infrastructure, while guaranteeing the desired level of isolation. In [117], an SDN-based solution is introduced to deploy multiple logical networks for different tenants. To this aim, the Flowvisor framework creates routing paths enforcing rules in the underlying network OpenFlow-based switches, according to each tenant's configuration. This feature can drastically limit the propagation and damages of security attacks between different network domains. An exemplary scenario of these security features is depicted in Fig. 6, where an SDN-based IoT access control application is implemented on top of the SDN controller to prevent the forwarding of undesired malicious traffic. In this way, each incoming/outcoming connection, directed to IoT domains, is verified according to predefined security policies. If the connection is allowed, the SDN controller issues relevant forwarding rules in the physical/virtual SDN switches along the desired networking path. On the other hand, malicious traffic generated by cybercriminals is blocked, by implementing the desired network access list. It is worth highlighting that the application domain of the SDN controller strictly depends on the network coverage under its responsibility. Even if in the case that the SDN

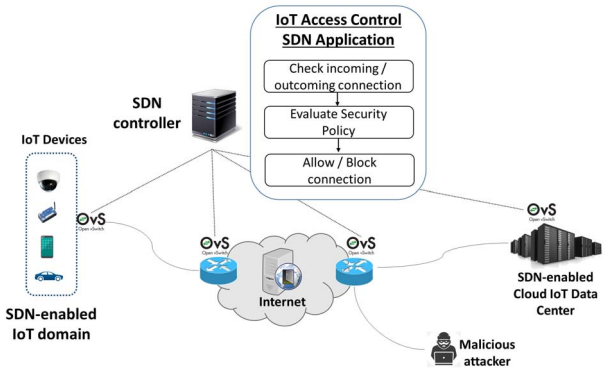


Fig. 6. SDN-based access control features in IoT domains.

controller supervises only the access network, the SDN-based security access control features can securely manage the traffic flows by specifying the IoT gateways' routes which provide connectivity for the attached IoT devices.

Furthermore, it can be used to dynamically separate malicious (or suspicious) network flows. In this vein, SDN-based separation solutions can offer different levels of network abstractions, so to appropriately separate network traffic and provide network views according to desired security properties. For securely interconnecting smart IoT environments, Boussard *et al.* [118] proposed SDN over federated local area networks, where communications among IoT devices are dynamically enabled according to requests from service users.

2) Security Network Monitoring Through Centralized Visibility: The SDN controller has a wide visibility of the data planes under its supervision and, through the control plane, can collect network status information by sending statistics query messages to the switches. In this way, the SDN controller can offer updated status of the underlying infrastructure and flow request messages to network applications running on the control plane. This approach can notably facilitate the development of strategies for implementing anomaly network analysis and detection of network-wide attacks. For example, several SDN-based strategies have been implemented to timely detect DDoS attacks [119], [120]. Since OpenFlow has been designed to provide flow-oriented status, Flexam [121] has been proposed to increase packet-level information by introducing a flexible sampling feature. This extension allows the SDN controller to define the sampling period according to either a probabilistic or a deterministic scheme, as well as the part of packets to select. This increased packet visibility can further support monitoring applications with low overhead. Moreover, the centralized view of the overall network can be exploited to better define monitoring analysis in complex scenarios. CloudWatcher [122] is an SDN-based framework which automatically detours network flows to guarantee that all necessary packets are inspected by pre-installed network security devices. In [123], SDN networking is exploited to determine optimal routing paths based on policy requirements and fixed-located security devices.

In the IoT landscape, an interesting idea is to extend the monitoring functions up to the extreme edge of the network, such as home device gateway and even IoT smart devices. This

can notably increase the potential offered by network-wide monitoring solutions leveraging a comprehensive vision of the network status. Indeed, performing network monitoring at line speed within the core network of Internet Service Providers (ISPs0 can be challenging accounting for the huge volume of flowing traffic. A complementary valid strategy is to exploit the capillarity of SDN-based home and enterprise routers. Indeed, SDN programmability ensures remote management and allows application to be easily updated as new security threats emerge. The advantages to perform anomaly detection mechanisms at the network edge have been experimentally proved in [124], where implemented detection algorithms, unable to satisfactorily identify anomalies at ISP level, present accurate detection rates for home and enterprise routers.

3) Dynamic Flow Control: A key feature of SDN is the capability of the SDN controller to dynamically install and update forwarding rules in network elements, so to appropriately manage traffic flows. This increased manageability notably raises the potential of network applications to implement appropriate security mechanisms. In [125], various SDN-based security functions (e.g., firewall and IDS/IPS) have been designed and implemented. For example, when an SDN switch does not have a flow rule to process a specific packet, a relevant request is forwarded to the controller which can decide the relevant packet processing based on specific application policies. This feature can enable a dynamic access control function, which is commonly implemented to protect a network according to the specified privileges and security policies.

Furthermore, the dynamic flow control can notably increase the potential countermeasures to cope with security threats, going beyond dropping packets. These defense solutions can include dynamic quarantine and network reflectors either for advanced analysis with honeypots or for forensics analysis. Indeed, by complementing SDN with IDS solutions able to discern suspicious and malign flows, the forwarding rules can be dynamically updated without requiring the use of specific proxies. Also, SDN features allow to notably improve the responsiveness of the security mechanisms deployment, better coping with network attacks. In this vein, various SDN-based schemes have been defined to face DDoS attacks [126], [127], which can drastically impact IoT system behavior.

The SDN-based flow management can be extremely useful for increasing the security of critical infrastructures, where vital data are exchanged among elements of Industrial Control Systems (ICS). In [128], an SDN-based architecture allows an ICS operator to forward replicas of sensitive traffic streams towards an IDS located in a strategic position to analyze as many traffic flows as possible. In this way, the ICS operator can instruct specific SDN network switches to duplicate traffic, for the streams that have to be monitored, and select optimal forwarding paths by exploiting spare bandwidth that might be available in over-provisioned networks. This approach is able to meet strict requirements in terms of packet loss for critical infrastructures.

4) Host and Routing Obfuscation: Malicious attackers leverage static network configuration to discover potential target vulnerabilities. Indeed, scanning tools and worms usually send probes to random IP addresses as precursory for many malicious vectors. To cope with these threats, SDN flexibility offers enhanced network manageability. Jafarian *et al.* [129] proposed a solution that mutates IP addresses of hosts with high unpredictability, so to maximize the distortion of attackers' network knowledge and increase the deterrence of attack planning. By leveraging SDN-based packet processing, the IP mutation is transparent to the end-host. Also, AnonyFlow [130] is an in-network anonymization service, which dynamically assigns temporary IP addresses to ensure user privacy. In this way, third parties on the Internet are unable to correlate user traffic and compose user profiles by observing specific IP addresses. A proof-of-concept prototype has been implemented using OpenFlow-based switches and has proved endpoint anonymity at line speed without compromising network performance.

Static forwarding routes can offer advantages to cybercriminals to carry out eavesdropping and DoS attacks on specific traffic flows. In [131], a proactive Random Route Mutation strategy is defined to enable dynamic change of forwarding paths, while preserving QoS end-to-end connectivity. SDN flexibility represents the ideal technology for developing and managing random routes, by appropriately updating flows in SDN-switches. To mitigate network analysis and interference analysis, BlackSDN has been proposed in [132], where IoT communications are protected by encrypting the header and the payload. Furthermore, the SDN controller operates as a trusted third party for securing routing and optimizing performance. The framework has been demonstrated for IEEE 802.15.4 networks, with devices operating with different duty cycles.

5) Security Network Programmability: The increased network programmability offered by the SDN controller can boost the development and deployment of security network applications. To this aim, the efforts towards the improvement of Northbound APIs and the definition of SDN-oriented coding languages can introduce several advantages to extend network functionalities [133]. In the context of security applications, the FRESCO framework [134] offers a scripting language to assist programmers in developing new SDN-based security mechanisms, by also leveraging different exemplary case studies. Furthermore, the framework also includes reusable modules which can be integrated to develop advanced security features. The FRESCO Application Layer prototype is implemented in Python, and operates as an OpenFlow application on NOX, by embedding a specialized security kernel, Fortnox [135], for the enforcement of relevant flows. However, the proposed approach is generic and can be ported to different SDN controllers.

Several works have also proposed some promising extensions of SDN control plane to increase the potential of SDN network applications. Avant-guard [136] has introduced two mechanisms, namely connection migration and actuation triggers. The former can drastically reduce the amount of control traffic in case of scanning and DDoS attacks, enabling greater scalability of centralized control. The latter has been designed to improve network monitoring services. These actuation triggers can be used to register for asynchronous call back and

add flow rules which are activated when specific conditions are identified. The combination of these two mechanisms allows to develop more scalable and resilient security services. The OFX framework exploits the computing capabilities of OpenFlow switches to deploy security applications within the network infrastructure. In particular, OFX [137] allows to install OFX software modules and carry out processing and monitoring tasks directly on the switches. This approach can notably increase the performance of SDN-based security applications by reducing the interactions between the data and control planes.

MEC scenarios, whereby intensive computing tasks are offloaded from mobile devices to (edge) cloud resources, represent an exemplary use case to demonstrate the opportunity to build security applications by leveraging SDN. These approaches are also appealing in enterprise contexts where business applications executed in mobile devices can improve enterprise operations. To meet the desired security levels, both performance, strict privacy, and trust requirements should be accounted for. This is particularly challenging in enterprise/campus networks where thousands of IoT devices executing different applications and with different privileges have to share the same physical and network infrastructure. In this vein, an Enterprise-Centric Offloading System (ECOS) [138] has been proposed to manage offloading by leveraging the enhanced SDN programmability. In particular, ECOS operates an application running on top of the SDN enterprise-wide controller to orchestrate all mobile application offloads using a simple, expressive policy language. Then, the ECOS framework enforces trust and privacy constraints by controlling the flows of traffic between mobile devices and selected computing resources, and by triggering additional higher-layer security mechanisms. Another exemplary effort for SDN-based IoT environments is represented by RolSec [139], a role-based security architecture, whereby the SDN controller is distributed according to its security roles. In this way, the architecture can provide extreme scalability by associating different controllers to different security features. The resulting solution is composed of three controllers: (i) Intrusion controller, which monitors the traffic, manages the routes for each flow, and provides secure routing; (ii) Key controller, which is a repository of both symmetric and asymmetric keys, handling their appropriate distribution; (iii) and Crypto controller, which provides cryptographic services, such as integrity, privacy, authentication, and identity management.

VI. NFV-Based Security Mechanisms in IoT

The adoption of virtualization technologies within network environments has recently changed the landscape of Telecommunication industries, leading to the NFV paradigm. Indeed, the decoupling of software from hardware can bring notably advantages for both capital and operating expenditures, increasing the manageability, scalability, and resilience of network function provisioning. Furthermore, the ability to deploy on-demand network solutions can notably accelerate in-network processing and ease the composition of integrated services.

A. Background on NFV Adoption for IoT Systems

ETSI NFV has played a main role towards the standardization of NFV approach, releasing several documents regarding architecture, use cases, guidelines for implementation. The ETSI NFV architecture [140] is composed of three main blocks, which are detailed hereunder.

The *Network Function Virtualization Infrastructure (NFVI)* includes both hardware and software components which are required to create the virtual environment for the execution of virtual functions. Commercial-off-the-shelves nodes provide processing, storage, and network capabilities which are abstracted through the virtualization layer. The computing and storage virtual resources may be provided in terms of virtual machines and containers, according to the implemented virtualization technologies, e.g., hypervisor and container engine, respectively [141]. On the other hand, virtual networks include virtual nodes, with either hosting or routing capabilities, and virtual links, which represent the logical interconnection of two virtual nodes, independently from the underlying physical network.

The *Virtual Network Functions (VNFs)* refer to the virtualized implementation of network functions with well-defined functional behaviour and external interfaces. VNFs are deployed over virtual resources, such as VMs and containers. A VNF can be also composed of multiple internal components, where each component can be hosted in a single VM or container and interconnected through appropriate virtual network interfaces. VNFs can be chained with other VNFs and/or physical network functions to implement a network service (NS). The order, type, and number of VNFs, which compose a NS, depends on the expected service functionality.

The increased flexibility introduced by virtualized network appliances, as well as the complexity of the underlying infrastructure, has demanded for novel management features. To this aim, ETSI NFV has designed a *Management and Orchestration (MANO)* framework which controls the efficient deployment of VNFs and it is composed of three main components:

- The Virtualized Infrastructure Manager (VIM) controls the hardware resources provided by the NFVI, as well as the relevant virtualization tools. Since NFVI can span across several physical locations, e.g., where NFVI Point of Presences (PoPs) are operated, the VIM is required to provide management over geo-distributed resources. Its tasks can also include collection of infrastructure information for monitoring, energy efficiency, fault, and performance analysis.
- The VNF Manager (VNFM) is responsible for the control of VNFs lifecycle, including the creation, configuration, maintenance, performance, and security management of VNF instances. A VNFM can be deployed either for each VNF or to serve multiple VNFs.
- The NFV Orchestrator (NFVO) has a central role in the framework by covering both resource and service orchestration. To this aim, the NFVO interacts with the VIMs to provide the resources necessary for hosting VNFs, and with the VNFM to manage the configuration of relevant VNFs.

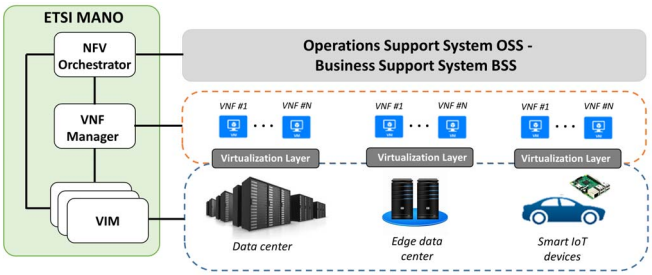


Fig. 7. Network Function Virtualization in IoT.

NFV can be also seen complementary to Edge computing, to deploy both software-driven network and application functions over the same virtualized infrastructure [142]. On the other hand, the IoT landscape introduces several challenges for the adoption of NFV paradigm, especially related to the resource constraints, the massive traffic requirements, and the mobility of IoT nodes. The evolution of lightweight virtualization technologies is tremendously impacting the NFV implementation, enabling the opportunity to deploy VNFs at the extreme edge of the networks [143], including IoT smart devices, as drawn in Fig. 7. In this vein, several works have proposed increasing the capabilities of IoT gateway to execute on-demand VNFs according to the application's requirements [144], [145]. Furthermore, the potential of hosting VNFs on top of smart IoT devices, such as smart cars [146], can open up the range of supported services providing fine-grained access to sensitive information and enhancing local data processing.

B. NFV Security Features in the IoT Ecosystem

The NFV paradigm can offer novel security strategies to cope with IoT vulnerabilities, especially accounting for the heterogeneity of IoT devices and their expected massive deployment. Indeed, Telco providers can extend the potential services offered to their customer including the Security-as-a-Service model [7], where prevention and defense mechanisms are provided on-demand. By adopting the NFV paradigm for IoT environments, several opportunities for enabling and efficiently orchestrating security enablers can be also introduced, as described in the following analysis of the key features of NFV-based security mechanisms. In this vein, the Cloud Security Alliance (CSA) has defined guidelines for cloud-delivered defence solutions, to assist enterprises and end-user to widely adopt this security paradigm shift [147]. The NFV approach presents remarkable advantages with respect to the hosting in remote cloud data centers, since the virtualized security functions can be deployed along the forwarding path, avoiding inefficient traffic detouring. In the following, we describe the main security features of the NFV paradigm for IoT systems. Similarly to the SDN security analysis provided in the previous section, our evaluation of NFV security features is complemented with the description of exemplary literature works, aiming to derive remarkable findings in the potential application of NFV-based security mechanisms to increase IoT protection.

1) Decoupling Security Software From Hardware: The basic principle of NFV deals with the opportunities to use commodity servers for deploying virtualized network functions, including security appliances, such as firewalls and DPIs. In this vein, [148] the APLOMB (Appliance for Outsourcing Middlebox) architecture has been introduced to offer network processing as cloud service. This system relies on the deployment of middleboxes as virtual instances over cloud infrastructures, and appropriate forwarding of the network traffic towards the virtualized instances. Furthermore, providing Deep Packet Inspection as a Service [149] for various security functions can lead to significant performance improvement.

The offloading of security functions to virtualized instances can be also extremely useful for IoT networks, accounting for the constraints of IoT devices. Furthermore, the offloading of security functions to external virtualized security functions can notably reduce the challenging problem of security administrator to implement the same level of protection over heterogeneous IoT devices. Cheng *et al.* [150] have introduced a framework aiming at blocking malware propagation by patching intermediate nodes, e.g., IoT gateways or access points, and securing infrastructure links. This scheme represents a more feasible solution instead of patching a broad range of resource-constrained IoT devices. By leveraging analysis on traffic patterns and IoT malware infection strategies, an efficient selection of the intermediate nodes to apply security patches can be carried out for ensuring timely mitigation of compromised IoT nodes.

Yu *et al.* [2] proposed an IoT security architecture, called IoTSec, envisioning customized micro-middleboxes, *μboxes*, which can be rapidly instantiated over lightweight platforms. The analysis in [151] aims at shedding light on the feasibility of container-based security solutions on resource-constrained edge nodes. The experimental assessment compares the native execution of security functions and their respective containerized counterparts. The results show an extremely low overhead of container-based security functions with respect to native execution, therefore supporting the provisioning of virtualized security functions even in constrained IoT environments. In [152], a new NFV-based security framework is proposed where virtualized security applications are instantiated in a user-specific Trusted Virtual Domain (TVD) in a network edge device. In this scenario, the trustworthiness of the TVD becomes essential since the security applications is executed on behalf of the user's devices and appropriate isolation mechanisms are required to guarantee the isolation between different users' security functions.

2) On-Demand Scalability and Fault Tolerance for Security VNF: By exploiting the dynamic instantiation of VNFs, network administrators can achieve a higher level of scalability and allow finer resource optimization. In this way, virtual security network functions can be scaled up/down according to the current workload of incoming traffic requests, as demonstrated in [148]. To optimize the auto-scaling procedure, it is essential to assess the impact of hardware and virtualization features on the VNF performance. Cao *et al.* [153] have proposed a framework, NFV-VITAL (Virtualization Impact on

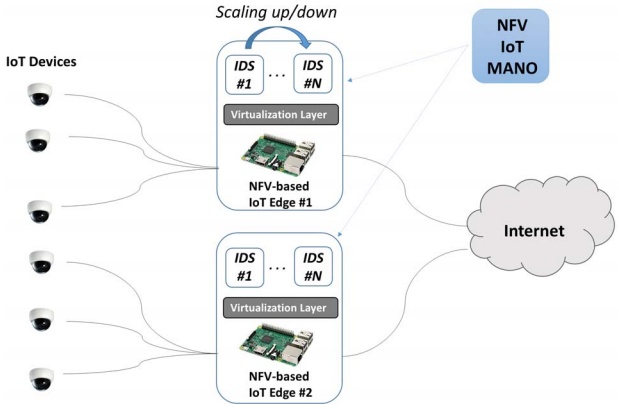


Fig. 8. Scaling features of security VNFs at the network edge.

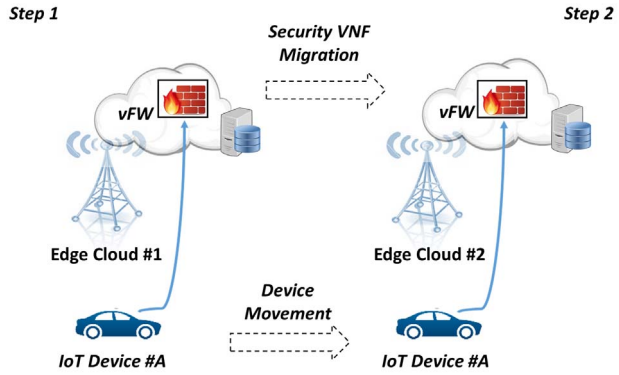


Fig. 9. Security VNF migration in mobile IoT environments.

Throughput and Load), for characterizing VNF performance based on user preference and available resources. The analysis of virtualized IDS solutions, such as Snort and Suricata, has demonstrated the benefits for selecting the optimal sizing and configuration. As shown in Fig. 8, the benefits of lightweight vitualization can guarantee the possibility to scale up/down security VNFs, such as IDS, according to traffic demands even at the network edge. The high scalability of virtual security instances allows to reduce the probability of dropping packets during network analysis and, thus, ensures high threat detection rate, independently from the traffic variations. This flexibility can be also enhanced by advanced orchestration of MANO-based IoT platform, able to balance the load of security VNFs over distributed edge nodes.

Another appealing feature, enabled by the virtualization technologies, deals with fault tolerance capability which can ensure the survivability of security functions. Several solutions are available to enable resilience and availability for cloud-based deployment [154]. In [155], state-aware replicas of virtual middleboxes are maintained, so that in case of a failure, a backup instance can be elevated to become master and handle the incoming traffic. There is an inherent trade-off in the number of replicas: this selection can depend on the criticality of the IoT security service to be guaranteed.

3) Mobility Support of Security VNF: Mobility represents a key feature for a broad range of IoT applications where IoT devices, such as wearables brought by human for continuous health monitoring and vehicular applications, can be always connected through different network access technologies. In this vein, the opportunity to instantiate virtualized network functions provides new flexibility in supporting the desired packet processing requirements near to the IoT device. This approach is well explained by the paradigm "Follow-me-edge" [156] where virtualized services can be seamlessly moved over different edge nodes to support manifold IoT applications with mobile devices [157], [158]. The proposed scheme represents an important solution for reducing core network traffic and ensuring ultra-short latency through a smart MEC architecture. In the context of security service offloading, the capabilities of seamlessly migrating virtualized security appliances is fundamental to guarantee the protection requirements, along the device mobility. This concept of VNF migration is represented in Fig. 9, where an instance of virtual Firewall is migrated between edge clouds according to the connected IoT device position, ensuring seamless protection even in mobile IoT environments [159]. In [160], a framework to support migration of virtual security instances near the end-user devices has been devised. The proposed approach leverages the use of virtualization technologies and SDN networking to manage the migration of security applications at the network edge, while minimizing the disruption of on-going connections. Furthermore, VNF migration can represent a potential strategy to cope with compromised underlying infrastructure [161]. Indeed, the decoupling from hardware can allow moving sensitive targets and network functions from a compromised node to another trusted environment.

4) Security Network Service Chaining: The increased flexibility of NFV paradigm allows improving the timeliness in the provisioning of services, as well as opens up a broader range of service composition accounting for fine-grained user requirements [162]. These advantages are also of notable interest for security domains where user traffic can be processed through chains of virtualized middleboxes, drastically reducing operational costs of network operators and improving resource utilization [163]. Furthermore, to carry out efficient security service chaining, SDN is complementary to NFV as it allows for highly elastic strategies to optimize traffic flows along the security VNFs chain, so to maintain end-to-end QoS. In Fig. 10, we report an illustrative example of joint SDN and NFV usage for security purposes in IoT environments. In particular, the traffic steering capabilities of SDN network are used to forward the traffic generated by (or directed to) IoT devices towards an NFV-based PoP, through a VXLAN tunnel, for security data processing. SDN is also used for NFV service chaining, steering the traffic through the security VNFs in the desired order by appropriately managing the routes in the SDN-controlled OVS switches. This joint adoption of SDN and NFV notably increases the flexibility in the implementation of the security policies by allowing dynamic instantiation of new security VNFs and appropriately modifying the IoT traffic routes.

In this vein, the SIMPLE framework [164] is an SDN-based policy enforcement framework which simplifies the traffic forwarding among middleboxes. In particular, SIMPLE

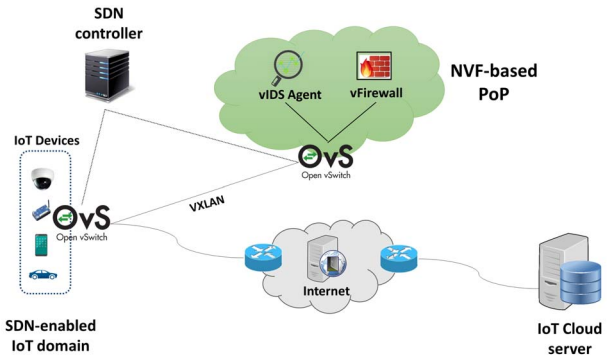


Fig. 10. SDN-based chaining of virtual security functions for IoT environments.

translates logical middlebox routing policy defined by the security administrators into forwarding rules, while accounting for the status of links and SDN switches, as well as middlebox resource constraints. As also remarked in [165], NFV flexibility requires appropriate network management to ensure that traffic is correctly forwarded when VNFs are either scaled or migrated, accounting for their internal states. To allow consistent reallocation of flows across VNF instances, OpenNF introduces a dedicated control plane to ensure coordinated control of both VNF states and network forwarding states. By leveraging specific APIs and primitives, the control plane can consistently move security VNF states along with dynamic flow management, with a low overhead in terms of VNFs development.

An initial promising example in the joint use of cloud-based security and SDN features is offered by Securebox [155] which aims at providing a composition of defense and management services for IoT systems, including device state configuration and traffic analysis. The platforms consists of two main components: (i) the Securebox frontend is a programmable gateway which uses SDN to dynamically configure the network flows for each attached device and to enforce the security policies; (ii) the Security and Management Service (SMS) is a cloud-based environment to deploy virtualized middleboxes according to the IoT security requirements. The SMS receives and analyzes the traffic flows from all the connected Securebox gateways. In this way, it can combine relevant analysis with updated knowledge (e.g., related to virus signature database) and provide enhanced detection solutions with respect to traditional network perimeter security systems.

VII. Lessons Learned in the Adoption of SDN/NFV-Based Security Solutions for IoT Systems

Due to the heterogeneity of IoT systems, the enforcement of appropriate security and privacy requirements is highly challenging. Conventional security solutions can hardly cope with the increasing security vectors against IoT. In this section, we discuss how the manifold features of SDN and NFV paradigms make these technologies the best candidates to complement conventional IoT security solutions in several aspects and bring notable advantages to increase the end-to-end protection of IoT systems. In Table II, we show how the combination of SDN and NFV can be leveraged to enhance security mechanisms for IoT devices. In particular, for each identified security enabler, we present the SDN/NFV-based counterparts and the IoT security threats which can be tackled accordingly.

Compared to traditional IoT solutions, scalability is one of the strongest aspects introduced by SDN and NFV. Offloading the extra processing required by security from either the gateways or the IoT devices to the network improves their energy efficiency and ensures more scalability to support the rising amount of traffic and functionalities. Moreover, thanks to the dynamic allocation of network and processing resources, virtual security appliances (e.g., vIDS, vDPI, and vFirewalls) can be scaled up/down according to the amount of traffic and to the number of attached IoT devices. We remark that NFV paradigm is strongly complementary to the security enablers developed so far, allowing to move from dedicated hardware to software instances. To further improve the performance, software-based security appliances can be refactored accounting for the latest micro-service development paradigm and cloud-oriented programming style [166], which promises to fully exploit the advantages offered by cloud environments in terms of scalability and reliability. On the networking side, the rise of IoT systems can be efficiently supported by the SDN infrastructure. Indeed, most of SDN controllers support distributed control planes, dynamic allocation of bandwidth, and OVS (Open Virtual Switches) ensuring optimal routing and improving the reactivity and availability of the network, even in case of security attacks.

SDN and NFV can be also the enabling key feature to deal with IoT management issues. Having a unified system, at different levels, is essential for IoT device management. To this aim, several works have been conducted to design SDN-enabled IoT gateways and sensors based on the Openflow protocol, OVS and programmable IoT applications [167], [168], as also discussed in Section V-A. This closes the gap between specific IoT device applications and network programmability. Having this level of flexibility does not only improve the resiliency of the infrastructure against failures, but also enables multi-level security enforcement. Indeed, SDN applications can implement stateless firewalls at the edge of the IoT network installing appropriate flows in the SDN physical/virtual switches. On the other hand, if the security policies require more advanced traffic filtering features, SDN can allow to reroute the traffic towards virtual stateful firewalls, deployed through NFV platform. This flexibility is extremely useful to satisfy the demanding and extremely granular security policies of IoT systems.

In an SDN environment, the SDN controller manages and supervises the entire network. Having a global vision of the network topology and real-time state allows the SDN controller to manage the network in an efficient way, ensuring the best routing decisions according to the desired Service Level Agreement (SLA). SDN is also capable of providing platforms for a wide range of different vendors and applications using multiple gateways and supporting multiple IoT devices [169], [170]. As a consequence, security administrators can use advanced mechanisms to control the network

TABLE II
COMPARISON OF CONVENTIONAL IoT SECURITY ENABLERS WITH SDN/NFV-BASED APPROACHES

Security Enabler	NFV	SDN	IoT Security Threats
Intrusion Detection System	Virtual Intrusion Detection System (vIDS) as a software instance on a cloud-enabled network.	Mirror the traffic to be analyzed by the vIDS using a secure data tunnel.	• Denial of Services attacks • Flooding attacks • Policy violation • Selective forwarding attacks • Sybil attacks • Abnormal network activities • Battery draining attacks
Firewall	Virtual Firewall (vFirewall) as a software instance on a cloud-enabled network.	Route the traffic through the vFirewall using a secure data tunnel.	• Access control • Port scanning • Denial of Services attacks • Fragmentation attacks • IP spoofing attacks
		SDN traffic flow management to operate as a stateless firewall.	
Deep Packet Inspector	Virtual Deep Packet Inspector (vDPI) as a software instance on a cloud-enabled network.	Mirror the traffic to be analyzed by the vDPI using a secure data tunnel.	• Spoofing attacks • Malicious code injection attacks • Abnormal network activities • Excessive bandwidth usage • Malformed network packets • IP spoofing attacks
Encryption	Virtual Encryption Proxy (vProxy) as a software instance on a cloud-enabled network.	Re-route the traffic to be analyzed through the vProxy using a secure data tunnel.	• Man-in-the-middle attacks • Eavesdropping attacks • Data alteration • Sniffing attacks • Impersonation attacks
		Create secure network tunnels for IoT data transport.	
Authentication and Authorization	Virtual Authentication, Authorization, and Accounting framework (vAAA) as a software instance on a cloud-enabled network.	Inject the relevant flow rules for each authenticated IoT device.	• IoT authentication inter-working • Service logging failures • Access control • User activity tracking
Security Service Function Chain (Security SFC)	Multiple security VNF instances (e.g., vDPi, vFirewall, and vIDS).	Manage the flows to and from the Security SFC using packet tagging.	• A combination of security threats (depending on the security enablers which are part of the implemented service chain).

behaviour according to the desired security policies. Moreover, virtual security appliances can be deployed in different environments, such as data centers, core networks, and IoT access networks with different configurations according to the underlying virtualization infrastructures [171].

IoT environments have to deal with rapid changes in the network to mitigate the growing number of security issues. It is not feasible for general users to manually configure each device to ensure the desired security properties. Having the latest security updates is mandatory and it should be handled by specialists. In this context, using SDN and NFV, administrators can maintain the security enablers up-to-date making it transparent to the end users. This also enables the feasibility of traffic-aware patching methodologies which can be extremely useful to address malware propagation, as elaborated in [150]. These patches can be provisioned and deployed at different levels of the infrastructure (i.e., core, edge and IoT networks) to ensure the protection of IoT solutions.

Moreover, in the context of self-defense, IoT devices are often low-energy devices which make their self-defense capabilities very limited. Offloading security features on higher performance hardware (cloud network servers) allows increased security standard protection, while saving device energy and manufacturing costs. In this context, resource intensive security appliances, such as DPIs, can really benefit from the extra available computation capabilities in cloud-enhanced network nodes. Finally, this extra performance flexibility enables function service chaining, which allows network operators to dynamically provide security features at different levels without requiring physical changes, either to the physical networks or to the IoT devices.

VIII. Open Research Areas

In this Section, we aim at defining the most promising research areas towards the broad deployment of SDN/NFV-based security solutions in IoT systems. Accounting for the complexity of IoT systems, our discussion aims at providing a comprehensive study of cutting-edge research efforts in these areas, so to cover the implementation of SDN/NFV-based security mechanisms at different levels, such as IoT access networks, core networks, and cloud/edge data centers. Our analysis covers the following research issues:

- the *definition of IoT security policies* introduces several challenges related to the level of abstraction in the security requirements, the formal language to be used for policy encoding, and contextual IoT aspects to be considered for an efficient use of SDN/NFV-based security mechanisms;
- the *orchestration of SDN/NFV-based security solutions over heterogeneous IoT environments* stimulates the research and development of appropriate federation schemes, so to seamlessly enforce innovative protection mechanisms across different technological and administrative IoT domains;
- the *inherent security of SDN and NFV frameworks* represents one of the main challenges towards the effective adoption of software-driven network security mechanisms, even more emphasized when considering the additional threats derived by the integration of IoT systems;
- the *optimal selection of SDN/NFV-based security mechanisms* can notably affect the experienced network and service quality, especially accounting for mission-critical IoT applications with stringent requirements in terms of latency and reliability, thus requiring novel analytical models and evaluation tools for security administrators;
- the *granularity of protection mechanisms* represents an open challenge in the provisioning of network slices tailored for IoT applications, considering the inherent trade-off among flexibility, performance, and cost.

These open issues are extensively discussed in the next subsections, to drive the research towards the effective realization of SDN and NFV-based security solutions able to ensure effective end-to-end IoT protection.

A. Policy Definition for SDN/NFV-Based IoT Security

Defining the security policies for IoT systems has a particular urgency due to the unification of physical and data domains, which can severely increase the risks of cyber attacks. To accelerate the path towards broad usability, IoT systems need to incorporate contextual policies definition (for consumers, enterprises, and public governments). The ultimate objective is to ensure an abstraction of high-level security requirements from one side and low-level configuration of security mechanisms from the other side. Allowing a higher degree of flexibility and manageability is strictly compelling for IoT involving the security of heterogeneous networks and devices. Indeed, expressing security requirements to govern distributed IoT systems represents a challenging task, especially when different administrative and technological domains are involved. To this aim, a Hierarchical Policy Language for Distributed Systems (HiPoLDS) [172] has been proposed focusing on decentralized service-oriented execution environments. HiPoLDS increases the abstraction of security policies in a concise and readable way, by allowing to specify the desired security properties along with the mechanisms to be implemented.

Similarly for SDN and NFV environments, several efforts towards security policies definition have been carried out. In [173], policy refinement for NFV environment has been defined through a double-step translation process. The security requirements are initially formulated in a High-Level Policies (HLP) language which follows the subject-object-attribute paradigm. By identifying the required security functions, the HLP policies are then translated in Medium-Level Policies (MLP) language which introduces an abstraction from the low-level details of potential VNF implementation. In the last step of policy refinement, MLP scripts are translated in specific VNFs' configurations to enable their effective instantiation. In [174], an OpenFlow-based security framework, OpenSec, has been proposed allowing a security administrator to specify and implement policies in human readable language. The policies include a description of the flow in terms of OpenFlow matching fields, security services to be applied to that flow (i.e., IDS), and strategies to react in case of a malicious threat is detected.

However, the specific features of IoT domain require also to extend policy definition accounting for contextual information, so to make relevant protection mechanisms more effective [2]. Security policies may also depend on the interactions among smart objects located in the same environment. All these aspects demand for empowering current policy templates to include the peculiarities of IoT systems, as well as the potential of novel software-driven security mechanisms.

B. Federation of Security Mechanisms Over Heterogeneous Domains

This research area tackles the issues related to the development of appropriate security tools which are adapted to the heterogeneous nature of IoT systems. Indeed, potential security mechanisms can be enforced at different levels, such as IoT access networks, core networks, and cloud/edge

environments. Furthermore, protection solutions for IoT can include a combination of conventional and novel IoT security approaches. In this context, the enforcement of SDN/NFV-based security mechanisms over different wired and wireless IoT ecosystems in a transparent way represents an open research challenge, with potentially great impact on the security implementation strategies. Indeed, interoperability is a core principle in IoT design and development, and its benefits should be also ensured in the security area. To this aim, it is worthwhile browsing the main recent efforts towards the orchestration of security mechanisms for NFV and SDN environments, as a basis for future enhanced IoT solutions.

Shin *et al.* [134] have proposed an OpenFlow security application development framework, FRESCO, to boost the rapid design of security applications. To this aim, different security detection and mitigation modules can be combined to fulfill the desired security requirements. Furthermore, the OrchSec framework has been proposed in [175] aiming at jointly utilizing network monitoring appliances and SDN control functions to develop security applications. The advantages of the proposed framework have been evaluated for a DNS amplification attack. Olivier *et al.* [176] have presented an SDN-based security architecture for IoT with multiple SDN domains where each domain can represent an enterprise network or a datacenter. Each domain is controlled by one or multiple SDN controllers and has its own security strategy. To allow a distributed enforcement of network security, this solution proposes the exchange of respective security requirements among domain SDN controllers. However, the east/westbound interfaces of SDN controller require further investigation, to fully ensure the security requirements over heterogeneous IoT domains.

With regard to the management of security in NFV environments, a Security Orchestrator has been devised in [177] to manage security over a hybrid Telco network, so to configure both physical and virtual network functions. Several responsibilities, such as Security Profile, Security Policy Management and Automation, and Trust Management, should be implemented in the Security Orchestrator to fully meet the end-to-end security. Furthermore, the interworking with current ETSI NFV MANO module has been described to coherently deploy physical/virtual security network functions. The ANSwer architecture [178] aims at combining VNFs and SDN features to deliver a set of strategies for network resilience, also accounting for potential security threats. The proposed architecture relies on a continuous monitoring of the network infrastructure and a feedback control-loop systems to timely provide remedial actions. The SELFNET architecture enriches SDN/MANO with self-management features for overall performance improvement in a fully autonomous way. Particular efforts are addressed to improve security features management and protect against malicious threats. Security VNF chains are dynamically adjusted and deployed across the networks by the autonomic management system. However, all the above-mentioned solutions do not specifically take into account IoT systems' characteristics to provide integrated security.

To address security IoT challenges, Choi and Kwak [179] have proposed the SDIoT security framework for the configuration of software-defined IoT environments. The approach combines SDN features with Big Data security analysis to provide a broad range of protection mechanisms for IoT devices. Besides, a reactive security framework [180], based on SDN and Service Function Chaining (SFC), has been specifically designed for industrial wind parks. After detecting potential security threats, the proposed solution can perform dynamic network reconfiguration, steering the malicious traffic towards specific security mechanisms, such as SCADA honeypots, tailored to the wind park operations. In [181] and [182], an architecture to orchestrate SDN, NFV, and conventional IoT security mechanisms has been proposed within the EU H2020 ANASTACIA project. In particular, the Security Orchestration plane aims at enforcing the deployment and configuration of physical/virtual security enablers in an automatic way. By also leveraging the outputs of Monitoring and Reaction components, the Security Orchestation plane can identify potential deviations from the required security policies and dynamically enforce appropriate countermeasures.

To sum up, in Table III, we report the main investigated security orchestration solutions for SDN/NFV, classifying them accounting for features in terms of policy support, integrated detection mechanisms, and autonomic reaction. Furthermore, since the integration of heterogeneous security mechanisms is crucial, we report the main supported enforcement environments: SDN, cloud, ETSI NFV MANO, and IoT. Indeed, still several efforts are required to develop appropriate federation schemes so to seamlessly enforce security mechanisms across different technological and administrative IoT domains. To this aim, the definition of open and standardized management interfaces also represents an essential step to provide a holistic view of end-to-end security over private and public IoT ecosystems.

C. Securing SDN-NFV Platforms

The security issues of both SDN and NFV are outside the scope of traditional security frameworks, because they involve securing the control planes that manage virtual resources and their relationships with applications and services. The adoption of virtualization technologies and SDN in Telco networks has introduced new potential security attacks which can potentially impact the efficiency of envisioned security approaches described in Sections V and VI. Furthermore, the extension of these paradigm to IoT ecosystems can even increase the risks accounting for the manifold heterogeneous connected devices and can cause more dramatical effects than in conventional networks. In the following subsections, we illustrate the security implications of emerging SDN/NFV-based networks for IoT, reporting the current state-of-the-art solutions and devising potential research directives.

1) SDN Threats for IoT Networks: SDN offers novel capabilities to monitor the traffic and adapt on-the-fly the network flows according to security demands. However, the increased flexibility and centralized control can generate

TABLE III
REVIEW OF SECURITY ORCHESTRATION PROPOSALS

Proposal	Features			Security Enforcement Domains			
	Policy-based orchestration	Detection	Autonomic reaction	SDN	Cloud	ETSI NFV MANO	IoT
Shin et al. [134]		+		+			
Lara et al. [174]		+		+			
Zaalouk et al. [175]	+	+	+	+			
Olivier et al. [176]				+			+
Jaeger et al. [177]	+					+	
Montero et al. [152]	+	+	+		+	+	
Machado et al. [178]	+	+	+	+	+	+	
Hafeez et al. [155]	+	+		+	+		+
Zhao et al. [161]	+	+	+	+	+	+	
Choi et al. [179]	+	+	+	+			+
Fysarakis et al. [180]	+	+	+	+			+
Molina Zarca et al. [182]	+	+	+	+	+	+	+

additional attacks [183]. We present a list of security threats based on the three main components of SDN networks, namely switches, controllers, and communication interfaces.

A first kind of security attacks concerns the failure of a SDN switch due to flow rule flooding, able to consume the whole flow table. This attack becomes extremely dangerous especially accounting for the resource constraints of SDN-enabled IoT devices. Malicious attackers can also attempt to either tamper flow rules for compromising the expected traffic flows or masquerading the legitimacy of a network element by leveraging spoofing approaches and the heterogeneity of IoT environments. A more severe attack deals with taking control of an SDN switch (i.e., hijacking) to compromise network behavior and infer confidential information within the system. Furthermore, in case of IoT environments, different wireless communication schemes, used for either control and data planes, can be targeted by security attacks. An increasing number of systems are also embracing software defined radios (SDRs) due to the several advantages in dynamic spectrum management, such as in Software Defined Vehicular Networks. Malicious configurations of SDR interface can lead to illegal use of relevant services, severely impacting the stability of network behavior, as investigated in [184].

The SDN controller embodies the network intelligence to manage the traffic flow forwarding, thus increasing the potential attractions of attackers since it represents a single point of failure. DoS attacks carried out by saturating the control links can dramatically impact the network performance, slowing down the request processing or making the SDN controller fully unavailable. Accounting for the capabilities to control the global infrastructure, network misconfiguration and flow tampering rules can be even more dangerous than similar attacks in SDN switches. For example, dynamic flow tunneling has the potential to orchestrate rules in such a way that no single rule violates any firewall setting, but they can jointly bypass security policies over inter-federated IoT environments. Finally, the hijacking of the SDN controller provides cybercriminals with extremely dangerous privileges to exploit the whole network for malicious purposes.

To ease programmability and management, the communication interfaces are fundamental to configure the network behavior in SDN networks. However, vulnerabilities in these communication channels can be exploited by attackers. Lack of encryption between SDN switches and relevant controller represents a remarkable risk to violate the confidentiality of interactions. Similarly, Man-In-The-Middle attacks can leverage weaknesses in trust mechanisms to impersonate the legitimate elements and tamper network configurations. The northbound interfaces between SDN controllers and applications suffer from lack of standardization and can represent a threat vector to trick or even manipulate the SDN controllers. Also, in case of federated IoT networks, the east/westbound interfaces among SDN controllers should be uniformly defined so to enable cross-boundary security policy enforcement and reduce potential vulnerabilities.

Different works have started to investigate and address some of these challenges [25], [26]. In this vein, Kreutz *et al.* [183] have suggested manifold approaches: (i) stringent authentication mechanisms and trust models to cope with common identity-based attacks; (ii) sandboxing techniques to isolate domains through well-defined interfaces that allow minimal set of operations; (iii) tamper-proof devices to securely store sensitive data. In [136], an extension of the data plane has been proposed to face the SDN saturation attacks that disrupt network operations as a consequence of scanning and DDoS attacks. FortNOX [135] has introduced a software extension for the NOX SDN controller to provide role-based authentication and security constraints enforcement by checking flow rules conflicts. In this way, FortNOX can identify malicious SDN applications which attempt to add flow rules aiming at circumventing secure traffic forwarding conditions. Li *et al.* [185] have investigated MitM attacks in IoT-Fog networks, highlighting the potential threats for IoT local area networks, by modifying flow tables, collecting information, and poisoning the controller's view. To efficiently detect MitM attacks, the authors have extended the OpenFlow protocol to incorporate Bloom filter mechanisms.

2) NFV Threats for IoT Networks: The possible security attacks for NFV-based networks can be categorized accounting for the logical blocks identified by the ETSI NFV architecture specifications.

The first potential security threat for virtualization infrastructure concerns the isolation failures, which can be carried out leveraging hypervisor and container engine vulnerabilities from one side, and network misconfiguration from the other side. The potential risks are even more augmented in IoT virtualized environments due to the heterogeneity of systems. Also, the opportunity to execute VNFs over third-party infrastructure opens up potential risks related to its trustworthiness. Indeed, a malicious administrator has the root access to the hypervisor and can violate data integrity and confidentiality of hosted VNFs, thus severely impacting their correct behavior. Indeed, accounting for the exponential increase of micro edge data centers, verification of their trustworthiness can be highly challenging [186]. Lack of monitoring for the underlying hardware resources represents a potential security flaw during the whole system lifecycle, from booting to run-time operations.

Further issues are related with the management and the deployment of VNFs over multiple environments. The exchange of relevant images, which contain all software components and configurations, can be intercepted by a malicious attacker, aiming to tamper the image in transit. Potential security threats for VNFs are also represented by their public interfaces, which can be attacked by external malicious entities, e.g., leveraging DDoS attacks. Furthermore, a compromised VNF can cause an avalanche effect, increasing the risk to compromise other VNFs involved in the same service chains and even other VNFs hosted in the same cloud environment, if appropriate isolation mechanisms are not adopted.

Accounting for the core roles in the orchestration of VNFs, the MANO modules represent the main target for any attacker since their hijacking can allow to control the remaining NFV components, e.g., by leveraging leakages in the authentication and authorization systems. Another crucial aspect deals with the misconfiguration of security policies, which can cause issues in the enforcement of security mechanisms according to the desired Service Level Agreement (SLA). As a result, malicious attackers can exploit any vulnerability to compromise deployed VNFs or other NFV MANO components. In this context, the fragmentation of VNFs represents a remarkable challenge in the enforcement of security policies over such a heterogeneous environment.

To face the above mentioned issues, the ETSI NFV security groups have released several specifications, providing guidelines in the management of security issues for NFV platforms. Several works in the literature have also investigated potential remediations against some of the above-mentioned issues. In [187], a security extension of NFV orchestrator has been proposed to enhance the capability of managing security mechanisms. To this aim, the TOSCA model has been extended to include security properties for each involved VNF. The template is then processed by a security policy engine which accordingly enforces relevant access control mechanisms. In [188], specific mechanisms to ensure VNF image integrity have been proposed for Telco networks. Besides, the VNF-Host sealing process has been devised to bind some VNF instances to a specific compute host which satisfies a set of system configuration policies. In [189], the NFVI Trust Platform (NFVI-TP) has been introduced by providing a root trusted module (RTM) to ensure every component built upon it is trusted. This middleware layer includes several trusted management components to verify the trustworthiness of security VNFs. Also, different NFVI-TPs can exchange trust information in a secure way to provide the reputation management system with appropriate feedback on VNFs performance. To tackle the issues of data confidentialiy and integrity in Telco cloud environments, an encryption service has been introduced in [190] to provide end-to-end protection between cloud hosts and among VNFs. Deng *et al.* [191] proposed a new framework for an effective provisioning and management of virtualized firewalls (vFW) to safeguard virtual networks. To this aim, they have defined a high-level firewall policy language, ensuring increased flexibility and mobility to protect VNFs, by leveraging features provided by both NFV and SDN. The VNGUARD framework transforms user policies to low-level firewall rules, then identifies an optimal placement, and adapts the configuration of the virtual firewall according to virtual network changes.

Despite the notable recent works to increase the security of NFV frameworks, further efforts are required to deal with scenarios where enhanced IoT access networks are fully integrated. The management of NFV platforms will need to ensure the protection and trustworthiness of executed VNFs not only in cloud-based Telco PoPs, but also on customer premise equipments and user equipments with virtualization capabilities, as discussed in Section VI-A. This can involve several issues in terms of reliable lightweight virtualization technologies, secure control protocols, and trust mechanisms suitable with the constraints of IoT nodes. Complementary to the security of SDN approaches, this represents a primary research area towards the effective adoption of software-driven security solutions for IoT systems.

D. Optimal Selection of SDN/NFV-Based Security Mechanisms

In this survey, manifold novel security mechanisms based on SDN and NFV have been examined for IoT systems. This increased variety of available solutions open up new challenges in the selection of the most appropriate security enablers. Indeed, some of the security mechanisms envisioned in Sections V and VI present some overlapping features, requiring further investigation to better evaluate the application scenarios and their potential integration with existing security solutions, especially accounting for the particularities of IoT systems. To evaluate the feasibility of SDN security mechanisms, Yoon *et al.* [125] have analyzed if SDN technologies can effectively enhance or replace the current security functions through the implementation of several representative SDN-based security functions (e.g., firewalls and network anomaly detectors). Their analysis in a realistic testbed has

provided useful insights on achievable performance, also highlighting the impact of hardware features in the overall results. Similar evaluation for security VNFs has been carried out in [192] and [193], where the performances of a firewall implemented as a virtual network function have been analyzed using off-the-shelves server.

Furthermore, the increased flexibility of NFV-based security provisioning introduces new challenging problems, such as which security services to implement, where to place and how to configure them [194]–[196]. This results in complex multi-dimensional optimization problem to determine the best allocation for virtualized security services. In [197], a preliminary model has been introduced considering three different actor perspectives: (i) users, who define the security requirements they need; (ii) developers, who specify the capabilities of their security applications, as well as the resource requirements to ensure desired performance; (iii) network operators, who are in charge of the cloud-based network topology and the relevant available resources to support security service provisioning. This model can be used to carry out an initial dimensioning of the system infrastructure, according to the expected number of customers and pre-defined security policies. The design of a run-time optimizer represents an even more challenging step since current workload should be accounted for in the reconfiguration of the security mechanisms, especially for the dynamic features of IoT systems. This on-demand adaptation can be triggered in the presence of mobile IoT devices which can change their access to the network, and in case of new identified security threats. We also remark that the provisioning of security should account for security-related best practices and recommendations [198]. Indeed, considering only the cost optimization in the chaining of virtual functions can lead to deployments which violate potential security patterns. This can be extremely complex especially in multi-domain IoT network infrastructures, where several security and trust criteria should be taken into account.

Last but not least, security mechanisms involve the consumption of extra resources which can impact the perceived QoS and cause a system performance degradation. In [199], the QoS^2 (Quality of Service and Security) framework is proposed to enable protection from malicious threats in an autonomous way, by dynamically relaxing or increasing security features. The framework is also able to adjust the level of security while ensuring acceptable QoS levels employing a Multi Attribute Decision Model approach. However, the research challenge related to the optimal selection of SDN/NFV-based security mechanisms is even more emphasized in IoT systems, where involved devices are characterized by resource constraints [200]. Therefore, the tuning of security mechanisms represents a key step to ensure the desired performance, especially accounting for the strict requirements of mission-critical IoT applications. In this vein, new analytical models and evaluation tools are required to assist network and service designers in the selection and optimization of SDN/NFV-based security mechanisms for IoT solutions.

E. Providing Customized Network Security With Network Slicing

The joint use of SDN and NFV also represents the basic foundations for more advanced management of network and application services within the network domain. In this vein, the concept of Network Slicing has recently attracted academia, industries, and SDOs such as 3GPPP and ITU. A "slice" is defined as an isolated set of programmable resources to implement network functions and application services through software programs for accommodating individual network functions and application services within each slice, without interfering with the other functions and services on coexisting slices [201]. This concept is extremely promising for the provisioning of IoT solutions which typically include multiple components deployed in distributed environments, as described in Section II. 5G network slices can provide end-to-end connectivity from IoT devices to cloud data centers and end-users while guaranteeing the desired performance [202]. Indeed, IoT applications are extremely variegated and present potentially conflicting security requirements. Accommodating IoT device security requests over the same physical infrastructure represents a complex task. Preliminary efforts have been conducted towards the provisioning of customized slices. PERMIT [203] aims at creating Virtual Mobile Network slices for specific verticals, taking into account inputs related to mobile service usage behaviour, perceived QoS, and mobility. In [204], 5G network slices customized for vehicle-to-everything services have been devised, involving vehicles exchanging data with each other, with the infrastructure and any communicating entity for improved transport fluidity, safety, and comfort on the road. However, security challenges have not been comprehensively investigated in the network slicing domain yet. An exemplary open challenge deals with the granularity of SDN/NFV-based protection mechanisms related to network slicing, accounting for the inherent trade-off among flexibility, performance, and cost. Indeed, slices and relevant security features can be provided: per vertical, per IoT tenant, per single device, and even per single application traffic flow. Further research efforts should be addressed to enable the creation and dynamic management of slices with different security mechanisms according to the specific IoT requirements.

IX. Concluding Remarks

The landscape of IoT is continuously evolving, attracting an increasing number of cybercriminals who aim at exploiting vulnerabilities of IoT systems to carry out malicious attacks on a potentially global scale. Conventional security mechanisms have been revealed to be inefficient accounting for the heterogeneity, pervasivity, and mobility of IoT devices. On the other hand, software-based networking and NFV are rapidly changing the Telco industry, encouraging a breakthrough also in the IoT security area.

In this survey, we first presented a broad overview on major security threats for IoT systems and conventional security countermeasures. Our analysis provides a thorough

investigation of the security features offered by both SDN- and NFV-based security mechanisms, analyzing the relevant state-of-the-art solutions for IoT systems. Our survey covers different potential deployment environments, such as IoT access networks, core networks, and cloud/edge data centers, illustrating how SDN and NFV security mechanisms can have a different impact on the end-to-end security of IoT solutions. Indeed, we discussed how the manifold features of SDN and NFV paradigms make these technologies the best candidates to complement conventional IoT security solutions, presenting for each identified security enabler the SDN/NFV-based counterparts. Through the lessons learned in the adoption of SDN/NFV-based protection approaches, we highlighted several advantages in terms of scalability, on-demand network programmability, energy efficiency, and mobility support. Since our literature review shows that the research in this area is still incipient, we also identified current open challenges related to SDN and NFV for IoT security: definition of security IoT policies, orchestration over heterogeneous IoT domains, inherent security of SDN and NFV systems augmented by IoT devices, optimal selection and deployment of SDN/NFV-based security mechanisms, and security granularity in network slicing. We hope and believe that this survey can provide extensive guidelines for new researchers who would like to explore this fervent arena.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] T. Yu, V. Sekar, S. Seshan, Y. Agarwal, and C. Xu, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proc. 14th ACM Workshop Hot Topics Netw.*, 2015, p. 5.

[3] M. Ambrosin, A. Compagno, M. Conti, C. Ghali, and G. Tsudik, "Security and privacy analysis of national science foundation future Internet architectures," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1418–1442, 2nd Quart., 2018.

[4] T. Taleb, "Toward carrier cloud: Potential, challenges, and solutions," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 80–91, Jun. 2014.

[5] T. Taleb, A. Ksentini, and R. Jantti, "'Anything as a service' for 5G mobile systems," *IEEE Netw.*, vol. 30, no. 6, pp. 84–91, Nov./Dec. 2016.

[6] T. Taleb *et al.*, "EASE: EPC as a service to ease mobile core network deployment over cloud," *IEEE Netw.*, vol. 29, no. 2, pp. 78–88, Mar./Apr. 2015.

[7] V. Varadharajan and U. Tupakula, "Security as a service model for cloud environment," *IEEE Trans. Netw. Service Manag.*, vol. 11, no. 1, pp. 60–75, Mar. 2014.

[8] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the Internet of Things," in *Proc. IEEE World Congr. Services (SERVICES)*, New York, NY, USA, 2015, pp. 21–28.

[9] R. H. Weber, "Internet of Things–New security and privacy challenges," *Comput. Law Security Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[10] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[11] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 8, no. 2, pp. 2–23, 2nd Quart., 2006, doi: 10.1109/COMST.2006.315852.

[12] Y. Zhou, Y. Fang, and Y. Zhang, "Securing wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 6–28, 3rd Quart., 2008.

[13] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2nd Quart., 2009.

[14] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[15] R. K. Pateriya and S. Sharma, "The evolution of RFID security and privacy: A research survey," in *Proc. Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, 2011, pp. 115–119.

[16] M. Saadeh, A. Sleit, M. Qatawneh, and W. Almobaideen, "Authentication techniques for the Internet of Things: A survey," in *Proc. IEEE Cybersecurity Cyberforensics Conf. (CCC)*, 2016, pp. 28–34.

[17] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, "Authentication protocols for Internet of Things: A comprehensive survey," *Security Commun. Netw.*, vol. 2017, Nov. 2017, Art. no. 6562953.

[18] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, Apr. 2017.

[19] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 3rd Quart., 2015.

[20] A. M. Nia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 4, pp. 586–602, Oct./Dec. 2017.

[21] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[22] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, pp. 10–28, Jun. 2017.

[23] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A survey of securing networks using software defined networking," *IEEE Trans. Rel.*, vol. 64, no. 3, pp. 1086–1097, Sep. 2015.

[24] S. Shin, L. Xu, S. Hong, and G. Gu, "Enhancing network security through software defined networking (SDN)," in *Proc. 25th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2016, pp. 1–9.

[25] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 325–346, 1st Quart., 2017.

[26] W. Li, W. Meng, and L. F. Kwok,, "A survey on OpenFlow-based software defined networks: Security challenges and countermeasures," *J. Netw. Comput. Appl.*, vol. 68, pp. 126–139, Jun. 2016.

[27] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2317–2346, 4th Quart., 2015.

[28] W. Yang and C. Fung, "A survey on security in network functions virtualization," in *Proc. NetSoft Conf. Workshops (NetSoft)*, 2016, pp. 15–19.

[29] M. D. Firoozjaei, J. P. Jeong, H. Ko, and H. Kim, "Security challenges with network functions virtualization," *Future Gener. Comput. Syst.*, vol. 67, pp. 315–324, Feb. 2017.

[30] S. Lal, T. Taleb, and A. Dutta, "NFV: Security threats and best practices," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 211–217, May 2017.

[31] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Gener. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.

[32] A. Sarac, N. Absi, and S. Dauzère-Pérès, "A literature review on the impact of RFID technologies on supply chain management," *Int. J. Prod. Econ.*, vol. 128, no. 1, pp. 77–95, 2010.

[33] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 757–789, 2nd Quart., 2015.

[34] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Comput. Netw.*, vol. 38, no. 4, pp. 393–422, 2002.

[35] S. A. Hamid, G. Takahara, and H. S. Hassanein, "On the recruitment of smart vehicles for urban sensing," in *Proc. Glob. Commun. Conf. (GLOBECOM)*, 2013, pp. 36–41.

[36] L. D. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[37] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.

[38] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV selection for a UAV-based integrative IoT platform," in *Proc. Glob. Commun. Conf. (GLOBECOM)*, 2016, pp. 1–6.

[39] M. R. Palattella *et al.*, "Standardized protocol stack for the Internet of (important) Things," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1389–1406, 3rd Quart., 2013.

[40] T. Taleb *et al.*, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.

[41] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, and J. Song, "Toward a standardized common M2M service layer platform: Introduction to oneM2M," *IEEE Wireless Commun.*, vol. 21, no. 3, pp. 20–26, Jun. 2014.

[42] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard 802.4-2011, 2011.

[43] J. Paradells, J. Oller, and C. Gomez, "Overview and evaluation of Bluetooth low energy: An emerging low-power wireless technology," *Sensors*, vol. 12, no. 9, pp. 11734–11753, 2012.

[44] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.

[45] M. R. Palattella *et al.*, "Internet of Things in the 5G era: Enablers, architecture, and business models," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 3, pp. 510–527, Mar. 2016.

[46] L. Militano, G. Araniti, M. Condoluci, I. Farris, and A. Iera, "Device-to-device communications for 5G Internet of Things," *EAI Endorsed Trans. Internet Things*, vol. 1, no. 1, 2015.

[47] A. P. Castellani, M. Gheda, N. Bui, M. Rossi, and M. Zorzi, "Web services for the Internet of Things through CoAP and EXI," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, 2011, pp. 1–6.

[48] J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, "A gap analysis of Internet-of-Things platforms," *Comput. Commun.*, vols. 89–90, pp. 5–16, Sep. 2016.

[49] J. Soldatos *et al.*, "OpenIoT: Open source Internet-of-Things in the cloud," in *Interoperability and Open-Source Solutions for the Internet of Things*. Cham, Switzerland: Springer, 2015, pp. 13–25.

[50] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Ed. MCC Workshop Mobile Cloud Comput.*, 2012, pp. 13–16.

[51] A. Mukherjee, H. S. Paul, S. Dey, and A. Banerjee, "ANGELS for distributed analytics in IoT," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, 2014, pp. 565–570.

[52] I. Farris *et al.*, "Social virtual objects in the edge cloud," *IEEE Cloud Comput.*, vol. 2, no. 6, pp. 20–28, Nov./Dec. 2015.

[53] R. Petrolo, R. Morabito, V. Loscrì, and N. Mitton, "The design of the gateway for the cloud of things," *Ann. Telecommun.* , vol. 72, nos. 1–2, pp. 31–40, 2017.

[54] R. Morabito, I. Farris, A. Iera, and T. Taleb, "Evaluating performance of containerized IoT services for clustered devices at the network edge," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 1019–1030, Aug. 2017.

[55] M. Chen, J. Wan, S. Gonzalez, X. Liao, and V. C. M. Leung, "A survey of recent developments in home M2M networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 98–114, 1st Quart., 2014.

[56] J. A. Guerrero-Ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and Internet of Things technologies," *IEEE Wireless Commun.*, vol. 22, no. 6, pp. 122–128, Dec. 2015.

[57] V. C. Gungor *et al.*, "A survey on smart grid potential applications and communication requirements," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 28–42, Feb. 2013.

[58] M. Memon *et al.*, "Ambient assisted living healthcare frameworks, platforms, standards, and quality attributes," *Sensors*, vol. 14, no. 3, pp. 4312–4341, 2014.

[59] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[60] J. P. Walters *et al.*, "Wireless sensor networks security: A survey," *Security Distributed, Grid, Mobile, and Pervasive Computing*. Boca Raton, FL, USA: Auerbach, 2007, p. 367.

[61] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Security Privacy*, 2005, pp. 49–63.

[62] X. Wang, S. Chellappan, W. Gu, W. Yu, and D. Xuan, "Search-based physical attacks in sensor networks," in *Proc. 14th Int. Conf. Comput. Commun. Netw. (ICCCN)*, 2005, pp. 489–496.

[63] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes: Real-world physical attacks on wireless sensor networks," in *Proc. Int. Conf. Security Pervasive Comput.*, 2006, pp. 104–118.

[64] M. H. R. Khouzani and S. Sarkar, "Maximum damage battery depletion attack in mobile sensor networks," *IEEE Trans. Autom. Control*, vol. 56, no. 10, pp. 2358–2368, Oct. 2011.

[65] D. R. Raymond, R. C. Marchany, M. I. Brownfield, and S. F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 367–380, Jan. 2009.

[66] X. Yang *et al.*, "Towards a low-cost remote memory attestation for the smart grid," *Sensors*, vol. 15, no. 8, pp. 20799–20824, 2015.

[67] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless LANs and countermeasures," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 7, no. 3, pp. 29–30, 2003.

[68] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 74–81, Jan./Mar. 2008.

[69] E. Bertino and N. Islam, "Botnets and Internet of Things security," *Computer*, vol. 50, no. 2, pp. 76–79, Feb. 2017.

[70] A. Mukaddam, I. Elhajj, A. Kayssi, and A. Chehab, "IP spoofing detection using modified hop count," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, 2014, pp. 512–516.

[71] Y.-Z. Li, Y.-B. Cho, N.-K. Um, and S.-H. Lee, "Security and privacy on authentication protocol for low-cost RFID," in *Proc. Int. Conf. Comput. Intell. Security*, vol. 2, 2006, pp. 1101–1104.

[72] B. Revathi and D. Geetha, "A survey of cooperative black and gray hole attack in MANET," *Int. J. Comput. Sci. Manag. Res.*, vol. 1, no. 2, pp. 205–208, 2012.

[73] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Netw.*, vol. 1, nos. 2–3, pp. 293–315, 2003.

[74] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proc. 3rd Int. Symp. Inf. Process. Sensor Netw.*, 2004, pp. 259–268.

[75] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2015, pp. 180–187.

[76] M. Abomhara and G. M. Køien, "Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Security*, vol. 4, no. 1, pp. 65–88, 2015.

[77] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," *IEEE Security Privacy*, vol. 9, no. 2, pp. 50–57, Mar./Apr. 2011.

[78] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 998–1010, 4th Quart., 2012.

[79] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 981–997, 4th Quart., 2012.

[80] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, 2014.

[81] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2015, pp. 1–6.

[82] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[83] T. Mamouni, J. A. T. Gijón, P. Olaszi, and X. Lagrange, "Universal AAA for hybrid accesses," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, 2015, pp. 403–407.

[84] J. L. Hernandez-Ramos, M. P. Pawlowski, A. J. Jara, A. F. Skarmeta, and L. Ladid, "Toward a lightweight authentication and authorization framework for smart objects," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 4, pp. 690–702, Apr. 2015.

[85] C. Rensing, M. Karsten, and B. Stiller, "AAA: A survey and a policy-based architecture and framework," *IEEE Netw.*, vol. 16, no. 6, pp. 22–27, Nov./Dec. 2002.

[86] D. Samociuk and B. Adamczyk, "Secure gateway for Internet of Things with internal AAA mechanism," *Theor. Appl. Informat.*, vol. 28, no. 3, pp. 17–35, 2017.

[87] R. K. Sharma, H. K. Kalita, and B. Issac, "Different firewall techniques: A survey," in *Proc. 5th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, 2014, pp. 1–6.

[88] N. Gupta, V. Naik, and S. Sengupta, "A firewall for Internet of Things," in *Proc. 9th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, 2017, pp. 411–412.

[89] H. Hasan *et al.*, "Secure lightweight ECC-based protocol for multi-agent IoT systems," in *Proc. IEEE 13th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, 2017, pp. 1–8.

[90] S. L. Keoh, S. S. Kumar, and H. Tschofenig, "Securing the Internet of Things: A standardization perspective," *IEEE Internet Things J.*, vol. 1, no. 3, pp. 265–275, Jun. 2014.

[91] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," in *Proc. 1st Annu. IEEE Commun. Soc. Conf. Sensor Ad Hoc Commun. Netw. IEEE (SECON)*, 2004, pp. 71–80.

[92] D. Díaz-Sánchez, R. S. Sherratt, P. Arias, F. Almenares, and A. M. López, "Proxy re-encryption schemes for IoT and crowd sensing," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, 2016, pp. 15–16.

[93] T. Sherasiya and H. Upadhyay, "Intrusion detection system for Internet of Things," *IJARIIE Int. J.*, vol. 2, no. 3, pp. 2344–2349, 2016.

[94] G. Kumar, K. Kumar, and M. Sachdeva, "The use of artificial intelligence based techniques for intrusion detection: A review," *Artif. Intell. Rev.*, vol. 34, no. 4, pp. 369–387, 2010.

[95] A. A. Gendreau and M. Moorman, "Survey of intrusion detection systems towards an end to end secure Internet of Things," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, 2016, pp. 84–90.

[96] R. T. El-Maghraby, N. M. A. Elazim, and A. M. Bahaa-Eldin, "A survey on deep packet inspection," in *Proc. 12th Int. Conf. Comput. Eng. Syst. (ICCES)*, 2017, pp. 188–197.

[97] D. H. Summerville, K. M. Zach, and Y. Chen, "Ultra-lightweight deep packet anomaly detection for Internet of Things devices," in *Proc. IEEE 34th Int. Perform. Comput. Commun. Conf. (IPCCC)*, 2015, pp. 1–8.

[98] "SDN architecture," Open Netw. Found., Palo Alto, CA, USA, Rep. TR-502, 2014.

[99] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for Internet of Things: A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1994–2008, Dec. 2017.

[100] F. Granelli *et al.*, "Software defined and virtualized wireless access in future wireless networks: Scenarios and standards," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 26–34, Jun. 2015.

[101] Z. He, J. Cao, and X. Liu, "SDVN: Enabling rapid network innovation for heterogeneous vehicular communication," *IEEE Netw.*, vol. 30, no. 4, pp. 10–15, Jul./Aug. 2016.

[102] R. D. R. Fontes, C. Campolo, C. E. Rothenberg, and A. Molinaro, "From theory to experimental evaluation: Resource management in software-defined vehicular networks," *IEEE Access*, vol. 5, pp. 3069–3076, 2017.

[103] T. Luo, H.-P. Tan, and T. Q. S. Quek, "Sensor OpenFlow: Enabling software-defined wireless sensor networks," *IEEE Commun. Lett.*, vol. 16, no. 11, pp. 1896–1899, Nov. 2012.

[104] B. T. de Oliveira, L. B. Gabriel, and C. B. Margi, "TinySDN: Enabling multiple controllers for software-defined wireless sensor networks," *IEEE Latin America Trans.*, vol. 13, no. 11, pp. 3690–3696, Nov. 2015.

[105] L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "SDN-WISE: Design, prototyping and experimentation of a stateful SDN solution for wireless sensor networks," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2015, pp. 513–521.

[106] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, "A software defined networking architecture for the Internet-of-Things," in *Proc. IEEE Netw. Oper. Manag. Symp. (NOMS)*, Kraków, Poland, 2014, pp. 1–9.

[107] *Open Network Operating System (ONOS)*. Accessed: Aug. 2018. [Online]. Available: https://onosproject.org/

[108] A.-C. G. Anadiotis, L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "Towards a software-defined network operating system for the IoT," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, 2015, pp. 579–584.

[109] C. Buratti *et al.*, "Testing protocols for the Internet of Things on the EuWIn platform," *IEEE Internet Things J.*, vol. 3, no. 1, pp. 124–133, Feb. 2016.

[110] P. Baronti *et al.*, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Comput. Commun.*, vol. 30, no. 7, pp. 1655–1695, 2007.

[111] I. Ishaq *et al.*, "IETF standardization in the field of the Internet of Things (IoT): A survey," *J. Sensor Actuator Netw.*, vol. 2, no. 2, pp. 235–287, 2013.

[112] J. Schulz-Zander, C. Mayer, B. Ciobotaru, S. Schmid, and A. Feldmann, "OpenSDWN: Programmatic control over home and enterprise WiFi," in *Proc. 1st ACM SIGCOMM Symp. Softw. Defined Netw. Res.*, 2015, p. 16.

[113] R. Trivisonno, R. Guerzoni, I. Vaishnavi, and D. Soldani, "SDN-based 5G mobile networks: Architecture, functions, procedures and backward compatibility," *Trans. Emerg. Telecommun. Technol.*, vol. 26, no. 1, pp. 82–92, 2015.

[114] N. Bizanis and F. A. Kuipers, "SDN and virtualization solutions for the Internet of Things: A survey," *IEEE Access*, vol. 4, pp. 5591–5606, 2016.

[115] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE Access*, vol. 5, pp. 1872–1899, 2017.

[116] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, to be published.

[117] R. Sherwood *et al.*, "FlowVisor: A network virtualization layer," OpenFlow Switch Consortium, Rep. 1132, 2009.

[118] M. Boussard *et al.*, "Software-defined LANs for interconnected smart environment," in *Proc. IEEE 27th Int. Teletraffic Congr. (ITC)*, 2015, pp. 219–227.

[119] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. IEEE 35th Conf. Local Comput. Netw. (LCN)*, 2010, pp. 408–415.

[120] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 602–622, 1st Quart., 2016.

[121] S. Shirali-Shahreza and Y. Ganjali, "Efficient implementation of security applications in OpenFlow controller with FleXam," in *Proc. IEEE 21st Annu. Symp. High Perform. Interconnects (HOTI)*, 2013, pp. 49–54.

[122] S. Shin and G. Gu, "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)" in *Proc. 20th IEEE Int. Conf. Netw. Protocols (ICNP)*, 2012, pp. 1–6.

[123] S. Shin, H. Wang, and G. Gu, "A first step toward network security virtualization: From concept to prototype," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2236–2249, Oct. 2015.

[124] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in *Proc. Int. Workshop Recent Adv. Intrusion Detect.*, 2011, pp. 161–180.

[125] C. Yoon *et al.*, "Enabling security functions with SDN: A feasibility study," *Comput. Netw.*, vol. 85, pp. 19–35, Jul. 2015.

[126] S. K. Fayaz, Y. Tobioka, and V. Sekar, "Bohatei: Flexible and elastic DDoS defense," in *Proc. USENIX Security Symp.*, 2015, pp. 817–832.

[127] N. Z. Bawany, J. A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," *Arab. J. Sci. Eng.*, vol. 42, no. 2, pp. 425–441, 2017.

[128] R. di Lallo *et al.*, "Leveraging SDN to monitor critical infrastructure networks in a smarter way," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, May 2017, pp. 608–611, doi: 10.23919/INM.2017.7987341.

[129] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "OpenFlow random host mutation: Transparent moving target defense using software defined networking," in *Proc. ACM 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 127–132.

[130] M. Mendonca, S. Seetharaman, and K. Obraczka, "A flexible in-network IP anonymization service," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2012, pp. 6651–6656.

[131] Q. Duan, E. Al-Shaer, and H. Jafarian, "Efficient random route mutation considering flow and network constraints," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2013, pp. 260–268.

[132] S. Chakrabarty, D. W. Engels, and S. Thathapudi, "Black SDN for the Internet of Things," in *Proc. IEEE 12th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, 2015, pp. 190–198.

[133] C. Trois, M. D. Del Fabro, L. C. E. de Bona, and M. Martinello, "A survey on SDN programming languages: Toward a taxonomy," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2687–2712, 4th Quart., 2016.

[134] S. Shin *et al.*, "FRESCO: Modular composable security services for software-defined networks," in *Proc. NDSS*, 2013.

[135] P. Porras *et al.*, "A security enforcement kernel for OpenFlow networks," in *Proc. ACM 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 121–126.

[136] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2013, pp. 413–424.

[137] J. Sonchack, K. Lazri, J. François, T. Delmas, and O. Festor, "Enabling practical software-defined networking security applications with OFX," in *Proc. NDSS*, vol. 16, 2016, pp. 1–15.

[138] A. Gember, C. Dragga, and A. Akella, "ECOS: Leveraging software-defined networks to support mobile application offloading," in *Proc. 8th ACM/IEEE Symp. Archit. Netw. Commun. Syst.*, 2012, pp. 199–210.

[139] K. Kalkan and S. Zeadally, "Securing Internet of Things (IoT) with software defined networking (SDN)," *IEEE Commun. Mag.*, to be published.

[140] "Network functions virtualisation (NFV); architectural framework V1.1.1," ETSI, Sophia Antipolis, France, Rep. ETSI GS NFV 002, 2013.

[141] R. Morabito, J. Kjällman, and M. Komu, "Hypervisors vs. lightweight virtualization: A performance comparison," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, 2015, pp. 386–393.

[142] V. Sciancalepore, F. Giust, K. Samdanis, and Z. Yousaf, "A double-tier MEC-NFV Architecture: Design and Optimisation," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2016, pp. 1–6.

[143] R. Cziva and D. P. Pezaros, "Container network functions: Bringing NFV to the network edge," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 24–31, Jun. 2017.

[144] B. R. Al-Kaseem and H. S. Al-Raweshidy, "SD-NFV as an energy efficient approach for M2M networks using cloud-based 6LoWPAN testbed," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1787–1797, Oct. 2017.

[145] N. Herbaut, D. Negru, G. Xilouris, and Y. Chen, "Migrating to a NFV-based home gateway: Introducing a surrogate VNF approach," in *Proc. IEEE 6th Int. Conf. Netw. Future (NOF)*, 2015, pp. 1–7.

[146] B. Baron *et al.*, "Virtualizing vehicular node resources: Feasibility study of virtual machine migration," *Veh. Commun.*, vol. 4, pp. 39–46, Apr. 2016.

[147] "Defined categories of service 2011 (SecaaS WG)," Cloud Security Alliance, Seattle, WA, USA, Rep., 2011.

[148] J. Sherry *et al.*, "Making middleboxes someone else's problem: Network processing as a cloud service," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 13–24, 2012.

[149] A. Bremler-Barr, Y. Harchol, D. Hay, and Y. Koral, "Deep packet inspection as a service," in *Proc. 10th ACM Int. Conf. Emerg. Netw. Exp. Technol.*, 2014, pp. 271–282.

[150] S.-M. Cheng, P.-Y. Chen, C.-C. Lin, and H.-C. Hsiao, "Traffic-aware patching for cyber security in mobile IoT," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 29–35, Jul. 2017.

[151] A. Boudi *et al.*, "Assessing lightweight virtualization for security-as-a-service at the network edge," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2018.

[152] D. Montero *et al.*, "Virtualized security at the network edge: A user-centric approach," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 176–186, Apr. 2015.

[153] L. Cao, P. Sharma, S. Fahmy, and V. Saxena, "NFV-VITAL: A framework for characterizing the performance of virtual network functions," in *Proc. IEEE Conf. Netw. Function Virtual. Softw. Defined Netw. (NFV-SDN)*, 2015, pp. 93–99.

[154] C. Colman-Meixner, C. Develder, M. Tornatore, and B. Mukherjee, "A survey on resiliency techniques in cloud computing infrastructures and applications," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2244–2281, 3rd Quart., 2016.

[155] I. Hafeez, A. Yi Ding, L. Suomalainen, A. Kirichenko, and S. Tarkoma, "Securebox: Toward safer and smarter IoT networks," in *Proc. ACM Workshop Cloud Assist. Netw.*, 2016, pp. 55–60.

[156] T. Taleb, S. Dutta, A. Ksentini, M. Iqbal, and H. Flinck, "Mobile edge computing potential in making cities smarter," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 38–43, Mar. 2017.

[157] A. Aissioui, A. Ksentini, A. M. Gueroui, and T. Taleb, "On enabling 5G automotive systems using follow me edge-cloud concept," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5302–5316, Jun. 2018.

[158] T. Taleb, A. Ksentini, and P. Frangoudis, "Follow-me cloud: When cloud services follow mobile users," *IEEE Trans. Cloud Comput.*, to be published.

[159] R. A. Addad, D. L. C. Dutra, M. Bagaa, T. Taleb, and H. Flinck, "MIRA!: A SDN-based framework for cross-domain fast migration of ultra-low latency 5G services," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, 2018.

[160] D. Montero and R. Serral-Gracià, "Offloading personal security applications to the network edge: A mobile user case scenario," in *Proc. IEEE Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, 2016, pp. 96–101.

[161] Z. Zhao *et al.*, "Autonomic communications in software-driven networks autonomic communications in software-driven networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2431–2445, Nov. 2017.

[162] H. Hantouti *et al.*, "Traffic steering for service function chaining," *IEEE Commun. Surveys Tuts.*, to be published.

[163] F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and O. C. M. B. Duarte, "Orchestrating virtualized network functions," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 4, pp. 725–739, Dec. 2016.

[164] Z. A. Qazi *et al.*, "SIMPLE-fying middlebox policy enforcement using SDN," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 27–38, 2013.

[165] A. Gember-Jacobson *et al.*, "OpenNF: Enabling innovation in network function control," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 4, pp. 163–174, 2014.

[166] N. Dragoni *et al.*, "Microservices: Yesterday, today, and tomorrow," in *Present and Ulterior Software Engineering*. Cham, Switzerland: Springer, 2017.

[167] Y. Li, X. Su, J. Riekki, T. Kanter, and R. Rahmani, "A SDN-based architecture for horizontal Internet of Things services," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2016, pp. 1–7.

[168] V. R. Tadinada, "Software defined networking: Redefining the future of Internet in IoT and cloud era," in *Proc. Int. Conf. Future Internet Things Cloud*, 2014, pp. 296–301.

[169] I. Miladinovic and S. Schefer-Wenzl, "A highly scalable IoT architecture through network function virtualization," *Open J. Internet Things*, vol. 3, no. 1, pp. 127–135, 2017.

[170] A.-C. G. Anadiotis, S. Milardo, G. Morabito, and S. Palazzo, "Towards unified control of networks of switches and sensors through a network operating system," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 895–904, Apr. 2018.

[171] M. Ojo, D. Adami, and S. Giordano, "A SDN-IoT architecture with NFV implementation," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2016, pp. 1–6.

[172] M. Dell'Amico *et al.*, "HiPoLDS: A hierarchical security policy language for distributed systems," *Inf. Security Tech. Rep.*, vol. 17, no. 3, pp. 81–92, 2013.

[173] C. Basile, A. Lioy, C. Pitscheider, F. Valenza, and M. Vallini, "A novel approach for integrating security policy enforcement with dynamic network virtualization," in *Proc. 1st IEEE Conf. Netw. Softw. (NetSoft)*, 2015, pp. 1–5.

[174] A. Lara and B. Ramamurthy, "OpenSec: Policy-based security using software-defined networking," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 1, pp. 30–42, Mar. 2016.

[175] A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, "OrchSec: An orchestrator-based architecture for enhancing network-security using network monitoring and SDN control functions," in *Proc. IEEE Netw. Oper. Manag. Symp. (NOMS)*, 2014, pp. 1–9.

[176] F. Olivier, G. Carlos, and N. Florent, "New security architecture for IoT network," *Procedia Comput. Sci.*, vol. 52, pp. 1028–1033, Jun. 2015.

[177] B. Jaeger, "Security orchestrator: Introducing a security orchestrator in the context of the ETSI NFV reference architecture," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 1255–1260.

[178] C. C. Machado, L. Z. Granville, and A. Schaeffer-Filho, "ANSwer: Combining NFV and SDN features for network resilience strategies," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2016, pp. 391–396.

[179] S. Choi and J. Kwak, "Enhanced SDIoT security framework models," *Int. J. Distrib. Sensor Netw.*, vol. 12, no. 5, 2016, Art. no. 4807804.

[180] K. Fysarakis *et al.*, "A reactive security framework for operational wind parks using service function chaining," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2017, pp. 663–668.

[181] I. Farris *et al.*, "Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2017, pp. 169–174.

[182] A. M. Zarca *et al.*, "Enhancing IoT security through network softwarization and virtual security appliances," *Int. J. Netw. Manag.*, Jul. 2018, Art. no. e2038, doi: 10.1002/nem.2038.

[183] D. Kreutz, F. M.V. Ramos, and P. Verissimo, "Towards secure and dependable software-defined networks," in *Proc. 2nd ACM SIGCOMM Workshop Hot Topics Softw. Defined Netw.*, 2013, pp. 55–60.

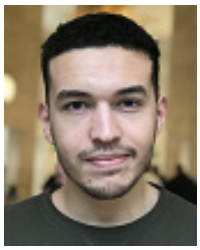
[184] A. Akhunzada and M. K. Khan, "Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues," *IEEE Commun. Mag.*, vol. 55, no. 7, pp. 110–118, Jul. 2017.

[185] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN infrastructure of IoT-fog networks from MitM attacks," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1156–1164, Oct. 2017.

[186] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog *et al.*: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.
[187] M. Pattaranantakul, Y. Tseng, R. He, Z. Zhang, and A. Meddahi, "A first step towards security extension for NFV orchestrator," in *Proc. ACM Int. Workshop Security Softw. Defined Netw. Netw. Function Virtual.*, 2017, pp. 25–30.
[188] S. Lal, S. Ravidas, I. Oliver, and T. Taleb, "Assuring virtual network function image integrity and host sealing in Telco cloue," in *Proc. IEEE ICC*, 2017, pp. 1–6.
[189] Z. Yan, P. Zhang, and A. V. Vasilakos, "A security and trust framework for virtualized networks and software-defined networking," *Security Commun. Netw.*, vol. 9, no. 16, pp. 3059–3069, 2016.
[190] S. Lal, A. Kalliola, I. Oliver, K. Ahola, and T. Taleb, "Securing VNF communication in NFVI," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2017, pp. 187–192.
[191] J. Deng *et al.*, "VNGuard: An NFV/SDN combination framework for provisioning and managing virtual firewalls," in *Proc. IEEE Conf. Netw. Function Virtual. Softw. Defined Netw. (NFV-SDN)*, 2015, pp. 107–114.
[192] L. A. F. Mauricio, M. G. Rubinstein, and O. C. M. B. Duarte, "Proposing and evaluating the performance of a firewall implemented as a virtualized network function," in *Proc. IEEE 7th Int. Conf. Netw. Future (NOF)*, 2016, pp. 1–3.
[193] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, "Virtual security as a service for 5G verticals," in *Proc. IEEE WCNC*, 2018, pp. 1–6.
[194] T. Taleb, M. Bagaa, and A. Ksentini, "User mobility-aware virtual network function placement for virtual 5G network infrastructure," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2015, pp. 3879–3884.
[195] M. Bagaa, T. Taleb, and A. Ksentini, "Service-aware network function placement for efficient traffic handling in carrier cloud," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2014, pp. 2402–2407.
[196] I. Benkacem, T. Taleb, M. Bagaa, and H. Flinck, "Optimal VNFs placement in CDN slicing over multi-cloud environment," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 616–627, Mar. 2018.
[197] C. Basile *et al.*, "Towards the dynamic provision of virtualized security services," in *Cyber Security and Privacy Forum*. Cham, Switzerland: Springer, 2015, pp. 65–76.
[198] A. S. Sendi, Y. Jarraya, M. Pourzandi, and M. Cheriet, "Efficient provisioning of security service function chaining using network security defense patterns," *IEEE Trans. Services Comput.*, to be published.
[199] T. Taleb and Y. Hadjadj-Aoul, "QoS^2: A framework for integrating quality of security with quality of service," *Security Commun. Netw.*, vol. 5, no. 12, pp. 1462–1470, 2012.
[200] C. Irvine, T. Levin, E. Spyropoulou, and B. Allen, "Security as a dimension of quality of service in active service environments," in *Proc. IEEE 3rd Annu. Int. Workshop Active Middleware Services*, 2001, pp. 87–93.
[201] A. Nakao, "Network virtualization as foundation for enabling new network architectures and applications," *IEICE Trans. Commun.*, vol. 93, no. 3, pp. 454–457, 2010.
[202] A. Nakao *et al.*, "End-to-end network slicing for 5G mobile networks," *J. Inf. Process.*, vol. 25, pp. 153–163, Feb. 2017.
[203] T. Taleb, B. Mada, M.-I. Corici, A. Nakao, and H. Flinck, "PERMIT: Network slicing for personalized 5G mobile telecommunications," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 88–93, May 2017.
[204] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G network slicing for vehicle-to-everything services," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 38–45, Dec. 2017.

Ivan Farris received the B.Sc. degree in telecommunications engineering, the M.Sc. degree in computer and telecommunications systems engineering, and the Ph.D. degree in information technology engineering from the University Mediterranea of Reggio Calabria, Italy, in 2011, 2013, and 2017, respectively. He is a Researcher with the Department of Communications and Networking, School of Electrical Engineering, Aalto University, Finland. His research interests include Internet of Things, edge computing, and network softwarization.

Tarik Taleb received the B.E. degree (with Distinction) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from Tohoku University in 2001, 2003, and 2005, respectively. He is currently a Professor with Aalto University, Finland, leading the MOSA!C Lab. He was a Senior Researcher with NEC Europe Ltd. until 2015. He was an Assistant Professor with Tohoku University, Japan. His research interests lie in the field of mobile core, mobile cloud networking, network function virtualization, software-defined networking, mobile multimedia streaming, and social media networking. He is an IEEE ComSoc Distinguished Lecturer.



Yacine Khettab received the master's degree in networking and distributed systems with the University of Science and Technology Houari Boumedinne, Algeria. He is currently a Research Assistant with the Department of Networking and Electrical Engineering, Aalto University. His current field of research focuses on providing security-as-a-service using SDN and NFV via different cloud-based orchestration techniques.

Jaeseung Song (SM'17) received the B.S. and M.S. degrees in computer science from Sogang University and the Ph.D. degree from the Department of Computing, Imperial College London, U.K. He holds the position of the oneM2M Test Working Group Chair and the TTA IoT/M2M Convergence Special Project Group Chair. From 2002 to 2008, he was with LG Electronics as a Senior Researcher leading the 3GPP SA Standard Team. He was with NEC Europe Ltd., as a leading standard Senior Researcher, from 2012 to 2013. He is currently an Associate Professor, leading the Software Engineering and Security Laboratory, Computer and Information Security Department, Sejong University. His research interests include software engineering, software testing, networked systems and security, with focus on the design and engineering of reliable IoT/M2M platforms, particularly in the context of semantic IoT data interoperability, secure software patch techniques, blockchain IoT, and edge computing.